ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA, CON BASE EN EL ESTÁNDAR ISO 27001, PARA LA EMPRESA NEGYSERT S.A., UNA PYME PRESTADORA DE SERVICIOS TECNOLÓGICOS BAJO MODALIDAD SAAS.”

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

MANUEL EDUARDO PAREDES HOLGUÍN

GUAYAQUIL – ECUADOR

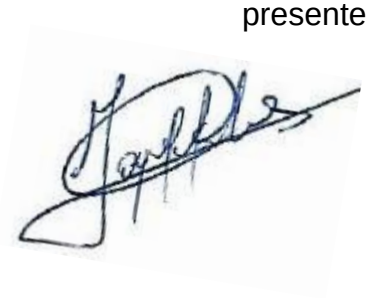
2021

AGRADECIMIENTO

Mi eterno agradecimiento a Dios, por haberme bendecido con la familia que acompaña mi andar, tan unida y tan dispuesta a arrimar el hombro unos por otros que suelo cuestionarme la existencia de otra igual.

A cada una de las personas que de una u otra manera han formado parte de este proceso, docentes, compañeros, personal administrativo y de apoyo de la maestría.

Un especial y merecido agradecimiento al equipo de NEGYSET S.A., por el apoyo incondicional para el desarrollo del presente trabajo.



DEDICATORIA

Dedico el presente a Dios, como base de absolutamente todo, y a mi amada familia. A mi adorada esposa, por acompañarme en cada paso, fomentar el crecimiento mutuo y haberme regalado tres bellos hijos.

A mis padres, a quienes amo y admiro intensamente, porque nunca han desmayado en su misión de ser una luz y guía en mi camino.

A mi hermana y su familia, por estar siempre presentes en los momentos de alegría, pero, aún más importante, nunca ausentarse en los momentos de dificultad.

Ing. Manuel Paredes H.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenin Freire Cobo

COORDINADOR MSIG

MSIG. Lenin Freire Cobo

DIRECTOR DE TRABAJO TITULACIÓN

MSIG. Robert Andrade Troya

MIEMBRO DEL TRIBUNAL

RESUMEN

El nivel de globalización que se vive en la actualidad ha sido artífice de la amplia aceptación de la que gozan los dispositivos tecnológicos electrónicos. Por otro lado, la creciente tendencia hacia la conectividad ha provocado que incluso los electrodomésticos comunes, como una televisión o una nevera, cuenten con una conexión hacia el internet.

En este contexto, las empresas no son una excepción en cuanto a la aceptación de la tecnología y la conectividad a través de internet, por el contrario, éstos se convierten en un punto de anclaje para apalancar el desarrollo de sus negocios y catapultar el crecimiento las empresas.

Pero este es solo el lado bueno de la moneda, en contraparte, este entorno desarrollado tecnológicamente y conectado a través de internet se convierte en un incentivo para la aparición y proliferación de la ciberdelincuencia, llevada a cabo por personas que buscan obtener algún beneficio económico, reconocimiento entre sus pares o incluso por simple satisfacción personal.

Con base a lo expuesto, el presente trabajo busca solventar la necesidad que tiene la empresa Negysert S.A., de contar con un esquema de seguridad de la información, basado en ISO 27001, que le permita minimizar la probabilidad de caer en alguna afectación por la actual falta de políticas al respecto y, por qué no, proyectarse hacia la obtención de certificación de la norma.

Para ello, será realizará un levantamiento completo de información, desde cero, empezando por los antecedentes, contexto y entono en el que Negysert S.A. desarrolla sus actividades, identificación de sus activos de información, hasta la definición de aplicabilidad de controles de seguridad, que permitan entregar como producto final el respectivo esquema de seguridad de la información

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BD Base de Datos

ISO Organización Internacional para la Estandarización

SI Sistema de Información

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

-

INTRODUCCIÓN

Considerando los vertiginosos volúmenes de información digital que producen las empresas en la actualidad, tanto estructurada como no estructurada, estos han pasado a considerarse como unos de los activos más importantes dentro de la organización, llamándose activos de información para ser precisos.

En tal virtud, es importante que las empresas implementen controles de seguridad a los activos tecnológicos relacionados con el ciclo de vida de la información, para que aseguren niveles adecuados de protección, procurando garantizar que la información mantenga sus criterios de integridad, confidencialidad y disponibilidad, de acuerdo a los privilegios que correspondan[1].

La aplicación de la norma ISO/IEC 27001:2013 permite la correcta identificación de la situación actual de las organizaciones, respecto a la implementación de políticas de seguridad de la información, y, a partir de esto, facilita la identificación de los activos de información, el análisis y tratamiento

de riesgos con el propósito de crear un esquema de seguridad para estos activos de información identificados en la empresa.

Una vez completada la implementación de la norma, las organizaciones gozan de los diversos beneficios que ésta trae con sigo, por ejemplo, procesos formalmente definidos, responsabilidades claramente definidas y asignadas, ligadas a la seguridad de la información, políticas y procedimientos estandarizados para asegurar la seguridad de la información, entre otros.

A lo anteriormente mencionados, se le puede añadir el posicionamiento que las organizaciones pueden obtener en el mercado comercial, una vez que lleguen a optar por la obtención de una certificación formal bajo la norma ISO/IEC 27001.

CAPÍTULO 1

1. GENERALIDADES

1.1. Antecedentes

Negysert S.A., Negocios y Servicios Triunfal S.A., es una PYME que fue fundada en el año de 2004 por el Ingeniero José Luis Paredes Espinel, con el objetivo de ganarse un lugar en el mercado empresarial mediante la oferta de un sistema de gestión empresarial, apuntando a madurarlo hasta convertirlo en un ERP (Enterprise Resource Planning) como tal.

Con el transcurso del tiempo y las varias implementaciones del sistema en diferentes nichos de mercados y líneas de negocio, éste fue consiguiendo la madurez y la robustez necesaria hasta que llegó a catalogarse formalmente como un ERP.

En el principio y por varios años más, el fuerte de la empresa era la implementación de su ERP bajo la modalidad de On-Premise, localmente en la infraestructura TIC de la empresa cliente. Esta modalidad tenía un buen índice de aceptación por parte del mercado, sin embargo, demandaba un considerable esfuerzo para cada nueva implementación, debido a la cantidad de ajustes personalizados que demandaba.

Con el transcurso del tiempo y con el objetivo de disminuir el costo de cada nueva implementación y, por ende, volverse más competitivo con respecto a productos parecidos en el mercado, la dirección de Negysert S.A. toma la decisión de priorizar o enfocar mayoritariamente sus esfuerzos en el modelo de negocio SaaS o “Software como un Servicio”.

De esta forma, bajo la modalidad SaaS, la empresa se encargó de levantar su infraestructura local, encargada de albergar de forma robusta a su solución ERP, y expuso un acceso en internet desde el que los clientes que suscriban el servicio puedan hacer uso de la solución comercializada por Negysert S.A.

1.2. Descripción del problema

A pesar de la madurez y experiencia ganada, a lo largo de los años de operación, por Negysert S.A., actualmente la empresa no cuenta con la definición de las respectivas políticas y procedimientos para garantizar la seguridad de la información.

Siendo que la mesa directiva, de la empresa, no es ajena a la realidad actual respecto a las distintas formas que pueden tomar las amenazas contra los activos de información y que, además, ha sido testigo de cómo dos de sus clientes han sufrido afectaciones en contra de estos activos, en los últimos meses.

Negysert S.A. se ha propuesto, como parte de sus objetivos estratégicos, tomar medidas al respecto de implementar un esquema de seguridad de la información, esquema que le permita ser más atractivos para sus clientes, especialmente en una nueva línea de negocios en la que están incursionando, relacionada con el relevamiento de datos y generación de estadísticas y tendencias.

Y, por qué no, con un esfuerzo adicional apuntar hacia la certificación formal bajo la norma ISO/IEC 27001.

1.3. Solución propuesta

Con base en los antecedentes expuesto, la solución propuesta en el presente trabajo se centra en la implementación de un esquema de seguridad de la información, basado en la norma ISO/IEC 27001:2013, con un enfoque en los procesos que componen la cadena de valor de la Negysert S.A.

Para lograrlo, se realizará el levantamiento y análisis de la situación actual de la empresa, que permita identificar si existe algún control o procedimiento que se esté aplicando respecto a la seguridad de la información.

Posteriormente se ejecutará la identificación de los activos de información, además de las principales amenazas relacionadas a éstos, y se complementará con un análisis de brechas, de tal forma que se pueda elaborar un documento de aplicabilidad, respecto a los controles propuestos como parte de la norma ISO/IEC 27001:2013.

1.4. Objetivo General

Diseñar un esquema de seguridad de la información, con base en el estándar ISO/IEC 27001:2013, para la empresa NEGYSERT S.A., con la finalidad de reducir las probabilidades de que ésta se convierta en víctima de un ataque cibernético exitoso.

1.5. Objetivos Específicos

- Analizar la situación actual de la empresa, respecto a la seguridad de la información.
- Identificar los activos de información de la empresa.
- Categorizar los activos de información de acuerdo a su nivel de criticidad.
- Identificar las amenazas a las que están expuestos los activos de información de la empresa.
- Analizar y valorizar las amenazas y riegos identificados.
- Diseñar las bases del esquema de seguridad de la información.

1.6. Metodología

Para el desarrollo del presente trabajo de titulación y como lo sugiere la norma, se realizará un trabajo enfocado en fases, de tal forma que cada fase termine con un entregable que represente una entrada o insumo para la siguiente.

De manera macro, las fases que se desarrollarán, como parte del presente trabajo, son las siguientes:

1. **Análisis de la situación actual de la empresa.**
    a. Esta fase debe permitir la identificación de los posibles controles y procedimientos, respecto a la seguridad de la

información, que podrían estarse aplicado de manera informal y los niveles de cumplimiento que estos representan según la norma.

2. **Identificación de los activos de información de la empresa.**
    a. De tal forma que sea posible limitar el alcance del esquema de seguridad de la información y los posibles controles que podrían aplicarse.
3. **Categorización de los activos de información.**
    a. En esta fase se categorizarán los activos de información de acuerdo a su nivel de criticidad para la cadena de valor de la empresa, procurando enfocar de manera correcta los respectivos controles a aplicar.
4. **Identificación de amenazas y riesgos**
    a. En esta fase se complementa todo el levantamiento realizado en las fases anteriores, clarificando las amenazas a las que están expuestos los activos de información, de acuerdo al modelo de negocio de la empresa.
5. **Análisis y valorización de las amenazas y riegos.**
    a. Con la finalidad de enfocar de mejor manera los esfuerzos y recursos de la empresa, es preciso valorizar las amenazas y riesgos identificados, procurando tomar medida sobre aquellos de mayor impacto.

6. **Diseño y documentación del esquema.**

    a. Finalmente, esta fase tomará todos los entregables de las fases anteriores y desarrollará el entregable final, el esquema de seguridad de la información según la norma ISO/IEC 27001:2013.

CAPÍTULO 2

2. MARCO TEÓRICO

2.1. Penetración de la tecnología en el mercado ecuatoriano

Es de conocimiento general, e incluso una situación evidente a simple vista, que la tecnología incrementa su presencia a nivel mundial de una forma vertiginosa. Ya no es para nada extraño encontrar que un niño pequeño, que aún no termina siquiera de aprender a caminar, ya tenga cierto nivel de experticia en el manejo de dispositivos como teléfonos inteligentes, tabletas y otros.

La población ecuatoriana no es ajena a dicha evolución tecnología, siendo así que, a pesar de las dificultades económicas o de accesibilidad, presenta un porcentaje muy importante respecto al acceso y uso de dispositivos tecnológicos y el internet.

Según [2], para el año 2015 el 66.7% de las empresas encuestadas, alrededor de 3.300 dentro de los rubros de manufactura, comercio, servicios y minería, dedican presupuesto para realizar inversiones en tecnologías de información y comunicación.

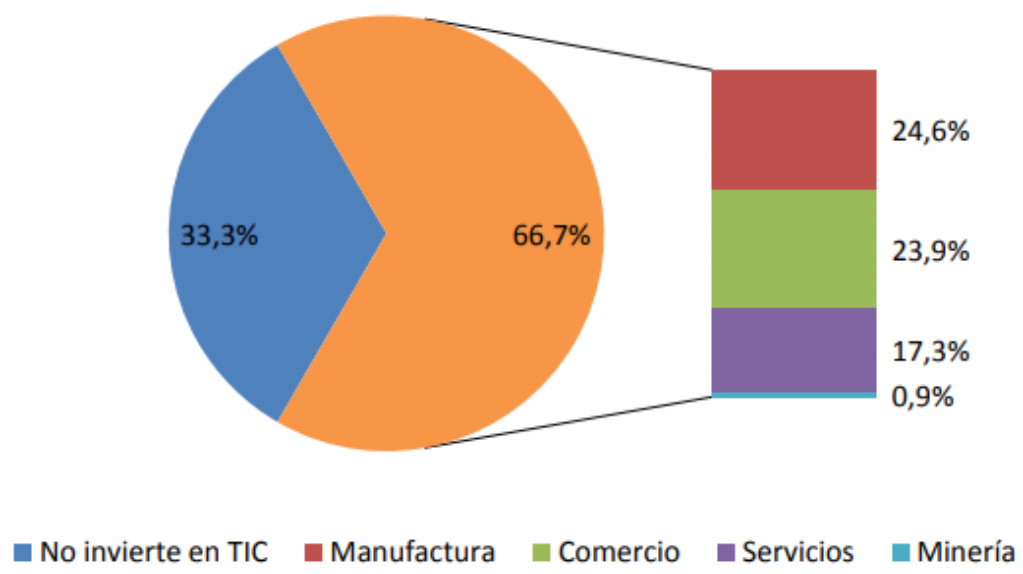


Figura 2.1 Porcentaje de empresas que realizan inversión en TIC, según sector económico [2]

De la misma forma, [2] reporta que, de las empresas encuestadas, el 98% cuenta al menos con una computadora de escritorio o con una notebook, como soporte para el desarrollo de sus actividades empresariales, además de otros posibles dispositivos tecnológicos.

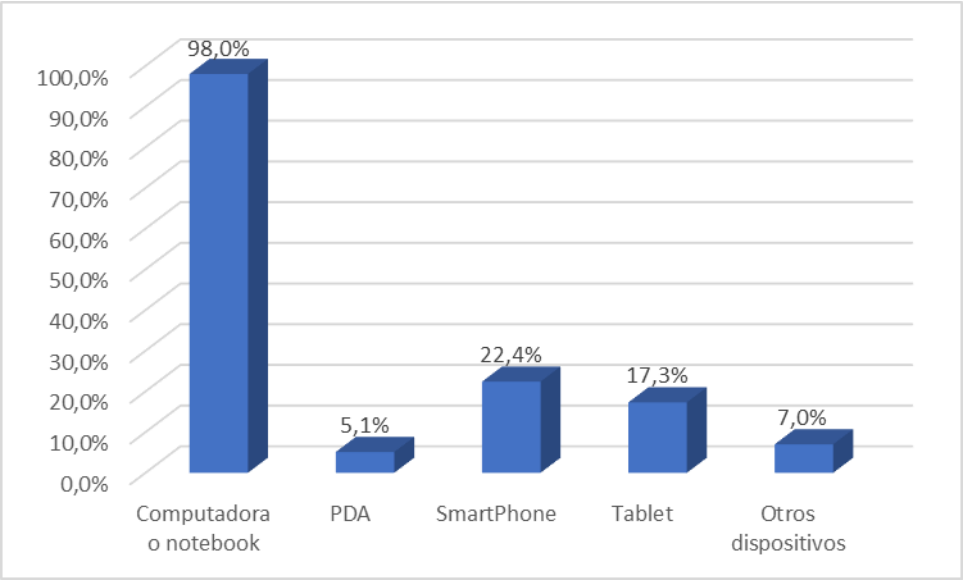


Figura 2.2 Tenencia de dispositivos tecnológicos [2].

En cuanto a la ciudadanía en general, [3] para el año 2018 reflejaba que un 43.74% de hogares urbanos contaba con al menos un computador, mientras su contraparte rural era del 23.27%. lo que promediaba un 37.43% a nivel nacional.

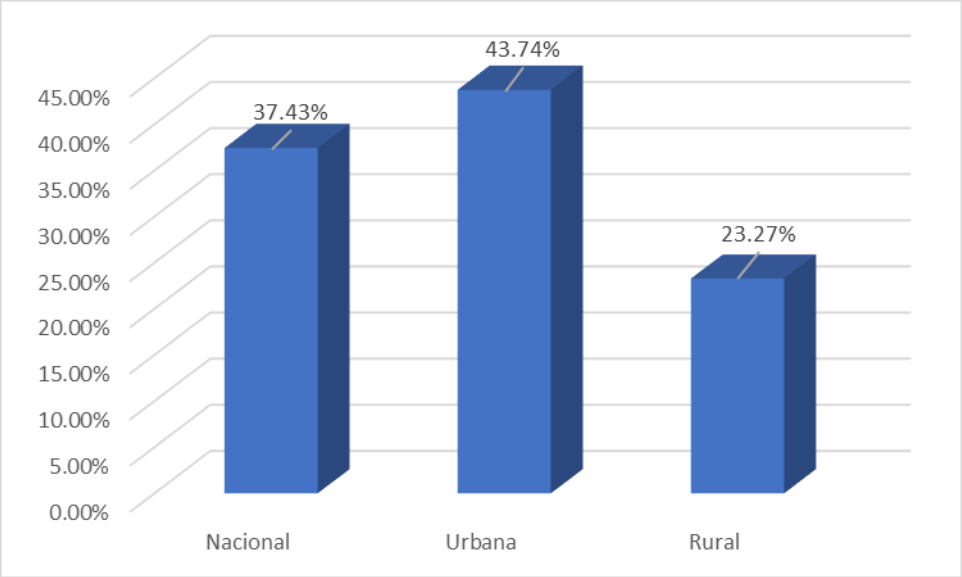


Figura 2.3 Porcentaje de hogares con al menos un computador [3].

Como complemento para el mismo año [3], el 46.56% de los hogares de la zona urbana y el 16.07% de los hogares de la zona rural contaban con acceso a internet, lo que promediaba un 37.17% de hogares con acceso a internet a nivel nacional.

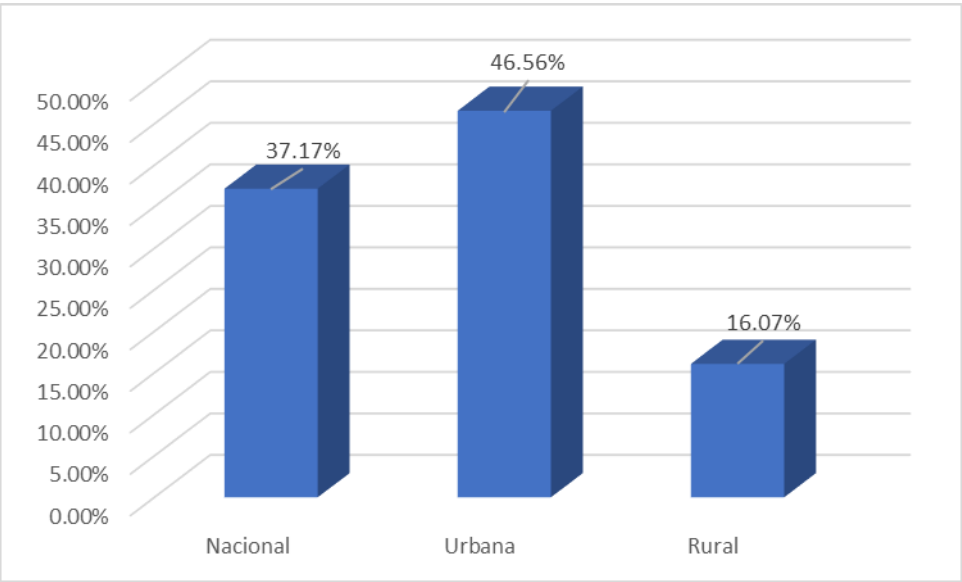


Figura 2.4 Porcentaje de hogares con acceso a internet [3].

Adicionalmente, se debe considerar que, para el presente año, debido a los estragos causados por la pandemia del COVID 19, los hogares ecuatorianos se vieron en la necesidad de realizar actividades de teletrabajo y educación virtual, por tal motivo, las estadísticas antes descritas muy seguramente se deben haber incrementado de forma estadísticamente significativa.

2.2. Seguridad informática

Se puede entender, como seguridad informática, a todos los esfuerzos realizados con la intención de definir, ejecutar, monitorear y mejorar las políticas, procedimientos, guías, reglas, etc., que buscan asegurar que los recursos informáticos, de una organización, permanezcan íntegros y resguardados de cualquier tipo de ataque o intrusión que pudiera comprometer la continuidad de la operación [4].

Es importante tener en cuenta ciertos conceptos básicos que permitan entender de una forma más clara el concepto y alcance de la seguridad informática, de forma macro:

- **Recursos informáticos**: todos los componentes de hardware y/o software, incluyendo también los repositorios de datos e información, involucrados en los procesos de cómputo y telecomunicaciones. A este conjunto también se lo puede identificar con el nombre de “activos informáticos”.

- **Vulnerabilidad: debilidad**, de un activo informático, que puede llegar a ser aprovechada por una amenaza, para su respectiva explotación.
- **Amenaza**: posible origen de eventos potencialmente dañinos para los activos informáticos de la organización.
- **Impacto**: medida o nivel del daño que se le puede vincular a una amenaza.
- **Riesgo**: medida combinada que se obtiene de la ponderación entre la posibilidad o probabilidad de que una amenaza se materialice, que suceda un evento dañino, y el posible impacto que podría significar para la organización.

Con base en lo expuesto, podemos concluir que el principal objetivo de la seguridad informática consiste en minimizar los riesgos relacionados a los activos informáticos de la organización, de forma que se pueda asegurar la continuidad del negocio, gestionando de manera eficiente los recursos necesarios para ello.

Complementariamente y de manera más enfocada en uno de los más importantes activos de las organizaciones en la actualidad, los activos de información, la seguridad de la información tiene un enfoque mucho más estratégico, antes que operativo (como lo hace la seguridad informática),

procurando asegurar los pilares fundamentales, la integridad, la confidencialidad y la disponibilidad de la información como tal [5].

Figura 2.5 Pilares fundamentales de la seguridad de la información
Fuente: Autor

Sirviéndose, para esto, de la ejecución constante de evaluaciones de los riesgos y amenazas ligados a los activos de información y generando, a partir de ello, planes de acción basados en normativas y mejores prácticas del mercado, procurando salvaguardar los activos de información de las organizaciones.

2.3. Estándares y normas en la seguridad informática

Sirviéndose, para esto, de la ejecución constante de evaluaciones de los riesgos y amenazas ligados a los activos de información y generando, a partir de ello, planes de acción basados en normativas y mejores prácticas

del mercado, procurando salvaguardar los activos de información de las organizaciones.

Entre dichos estándares se pueden mencionar los siguientes:

- **ITIL** – Biblioteca de Infraestructura de Tecnologías de Información.
- **COBIT** – Objetivos de Control para las Tecnologías de la Información y Relacionadas.
- **ISO/IEC 15504** – Determinación de la Capacidad de Mejora del Proceso de Software.
- **ISO/IEC 20000** – Calidad de los Servicios de TI.
- **ISO/IEC 27001** – Sistemas de Gestión la Seguridad de la Información.

ITIL puede definirse como un conjunto de buenas prácticas, recomendadas para la gestión y administración de los servicios relacionados con las tecnologías de la información, mismas que ayudan a que la organización desarrolle sus actividades orientando los esfuerzos correspondientes hacia el aseguramiento de la calidad de los servicios de TI [6].

Al día de hoy, ITIL se encuentra en su cuarta versión, misma con la que trata de responder de forma más adecuada a los constantes cambios y el

nivel de agilidad con el que las organizaciones, y por ende los servicios tecnológicos, desarrollan sus operaciones [7].

En esta nueva versión, ITIL se divide en los conceptos principales de “Sistemas de Valor de Servicio” (“Service Value Systems”) y “Flujos de Valor de Servicio” (“Service Value Streams”), dejando atrás el modelo de ciclo de vida que lo caracterizaba como un “Sistema de Gestión de Servicios” (SMS) y pasando a ser un “Sistema de Valores de Servicios” (SVS) concentrado en los siguientes 5 componentes principales del “Service Value” [8]:

- La cadena de valor del servicio ITIL
- Las prácticas ITIL
- Los principios guía de ITIL
- La gobernanza
- La mejora continua

COBIT se define como un marco de trabajo para la gobernanza y la administración de la tecnología y la información empresarial, con un alcance transversal a lo largo de la organización. Para el marco de trabajo, la tecnología y la información empresarial hacen referencia a absolutamente todos los dispositivos tecnológicos y toda la información que la organización procesa, sin importar el departamento en que esto

suceda, siempre y cuando representen un apoyo a la consecución de los objetivos empresariales [9].

Consecuentemente, la tecnología y la información empresarial no se limita de forma exclusiva al departamento de TI, pero por supuesto que incluye a éste.

La “Asociación de Auditoría y Control de Sistemas de Información”, ISACA por sus siglas en inglés, liberó una versión actualizada del marco de trabajo en el año 2019, está versión fue denominada como COBIT 2019. Entre los principales cambios se destaca su orientación o alineamiento con DevOps, la sustitución de los procesos basado en ISO-33000 por el modelo de capacidad CMMI y la inclusión del concepto de enfoque por áreas específicas, volviendo más flexible y práctica la adopción de COBIT [9].

La norma **ISO/IEC 15504** – Determinación de la Capacidad de Mejora del Proceso de Software, también conocida como SPICE por sus siglas en inglés, propone un modelo que puede ser utilizado para realizar la evaluación sobre las capacidades que describen a los procesos de desarrollo de software dentro de la organización. La norma también determina los requisitos necesarios para la ejecución de la evaluación de procesos referentes a cada una de las fases que comprenden el ciclo de

vida del software como tal, así como para desarrollo de los servicios que son provistos por las TIC [10].

La norma cuenta 10 componentes, que han sido publicados entre el 2003 y el 2011, enumeradas del 1 al 10. De estas partes, 8 se consideran como material de apoyo o anexos que pueden servir como guía de consultas para la implementación de los requisitos considerandos dentro de los componentes 3 y 7, mismos que constituyen el cuerpo normativo [10].

La norma **ISO/IEC 20000** – Calidad de los Servicios de TI, se orienta hacia la agrupación de las mejores prácticas internacionales en cuanto a la administración de servicios de TI respecta. Resaltando que se debe entender como servicios de TI a todos aquellos servicios cuya provisión está soportada en las tecnologías de la información. En este contexto, la norma no hace diferenciación entre los servicios provistos a los clientes externos y los provistos a los clientes internos [11].

Esta norma está compuesta por 8 secciones, de las cuales son la sección 1 y la 2 las más utilizadas por detallar los requisitos y proveer una guía para la correcta implementación y certificación formal bajo ISO/IEC 20000. Adicionalmente, su proceso de establecimiento y mejora continua se apoya en el ciclo PDCA.

Una buena forma de diferenciar esta norma respecto a lo que ofrece ITIL es teniendo claro que ISO/IEC 20000 se orienta hacia “lo que se necesita

hacer”, por otra parte, ITIL se enfoca en “como lograrlo”. Adicionalmente, se conoce que ISO/IEC 20000 se puede implementar de forma aislada, por si sola, sin embargo, los resultados que se obtienen al implementarla de forma conjunta con ITIL son claramente superiores [12].

Por su parte, **ISO/IEC 27001** – Sistemas de Gestión de la Seguridad de la Información, es una norma de reconocimiento y aceptación internacional, que brinda lineamientos y mejores prácticas que, siendo bien implementadas, permiten asegurar los 3 pilares fundamentales en cuanto a los datos, la información y los activos relacionados con su procesamiento, la disponibilidad, la integridad y confidencialidad [13].

ISO/IEC 27001, cuya última versión fue liberada en el año 2013 y fue revisada y confirmada en el año 2019, forma parte del conjunto de normas agrupadas dentro de ISO/IEC 27000. Respecto a la gestión de seguridad de la información, la norma ISO/IEC 27001 provee los requisitos que debe cumplir un sistema de gestión de seguridad de la información (SGSI) mientras, por su parte, la norma ISO/IEC 27002 provee un conjunto de buenas prácticas y de objetivos de control que se recomiendan implementar [14].

De manera resumida, la norma se enfoca en proveer medidas que ayuden a las organizaciones a asegurar la protección adecuada de los datos e información, sin importar el formato en que estos se presenten, así como

los activos involucrados en su, producción, tratamiento, transmisión y almacenamiento. Así mismo, los requerimientos de la norma son genéricos, de tal forma que esta puede ser aplicada en organizaciones de todo tipo, tamaño o línea de negocio [15].

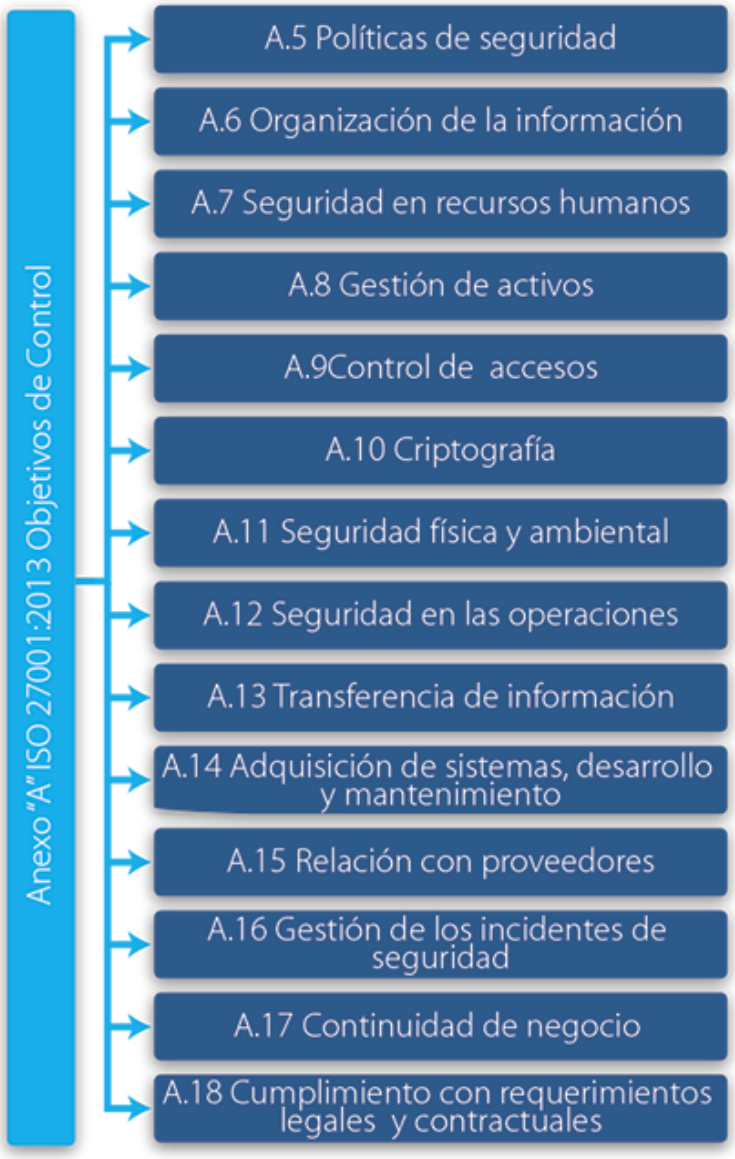


Figura 2.6 Dominios Anexo "A" de ISO 27001:2013 [16]

Entre los principales cambios que la norma experimentó, con la publicación de la versión 2013, se pueden destacar los ajustes a la estructura de los objetivos de control, pasando de 11 a 14 apartados, como se refleja en la imagen 2.6. De la misma forma, se ajustó el contenido de los controles que conforman el anexo A, pasando de 133 a 114 controles [17].

A continuación, se resume en contenido de cada uno de los 14 apartados o secciones que componen la norma ISO/IEC 27001 [18]:

A.5: Políticas de Seguridad de la Información: provee los controles relacionados con la forma de redactar que debe utilizarse para la definición y revisión de las políticas de seguridad.

A.6: Organización de la Seguridad de la información: en este apartado de tratan los controles respecto a la correcta designación de responsabilidades. Adicionalmente, se incluyen los controles que deben ser aplicados sobre el uso de dispositivos móviles y cuando se cuenta con una figura de trabajo remoto o teletrabajo.

A.7: Seguridad de los Recursos Humanos: hace referencia a los controles que deben aplicarse sobre todas las tareas que componen el proceso de contratación o vinculación de personas, incluyendo aquellas que se ejecutan previa y posteriormente al proceso, durante el tiempo en que las personas estén vinculadas a la organización y el correspondiente proceso de desvinculación.

A.8: Gestión de Activos: provee los controles necesarios con respecto a los inventarios de activos de información de la organización y su respectivo uso aceptable y su proceso de devolución. Así mismo, provee guías para la clasificación de la información de la organización, así como la gestión de los distintos medios utilizados para su almacenamiento.

A.9: Control de Acceso: guía para la definición de políticas de control y monitoreo de accesos, que se confieren a los usuarios, hacia la información, la red y los servicios de red, en todas sus formas, ya sea a través de sistemas, aplicaciones o cualquier otro medio que se utilice para el almacenamiento y procesamiento de la misma.

A.10: Criptografía: provee controles relacionados con los gestión y aplicación de métodos de codificación o encriptación de la información, especialmente aquella considerada de alta sensibilidad, por ejemplo, las claves de usuario. De esta forma, se pretende asegurar que, en caso de que exista una intrusión a las fuentes de información, se reduzca la posibilidad de que la confidencialidad y la integridad se vean comprometidas.

A.11: Seguridad física y del Entorno: este apartado hace referencia a los controles necesarios para prevenir los accesos físicos, no consentidos, en todas aquellas zonas que se hayan designado como “áreas seguras”,

procurando prevenir robos, daños o manipulaciones que puedan llegar a comprometer la continuidad de las operaciones de la organización.

Paralelamente se hace mención a los factores externos que pudiesen ocasionar daños o pérdidas, como eventos terroristas o de la naturaleza, como inundaciones, incendios, entre otros.

A.12: Seguridad de las Operaciones: provee lineamientos y controles referentes a las operaciones diarias de la organización, tanto para la administración de ambientes de desarrollo de software (desarrollo, pruebas, pre producción, producción) así como para la protección de los equipos informáticos de los colaboradores (sistemas operativos, instalación de actualizaciones, parches, aplicaciones, antivirus) y el respaldo de la información generada en el dicho proceso.

También se incluyen controles relacionados con las auditorias que se deben efectuar a los sistemas y aplicaciones que se utilizan como parte del desarrollo de las operaciones de la organización.

A.13: Seguridad de las comunicaciones: se contemplan los controles enfocados en el aseguramiento y protección de las comunicaciones de la organización, tanto a través de las redes internas como de las externas. Se enfoca en proteger toda transmisión de información que realice la organización, así como la segregación y asignación de accesos para los servicios expuestos en la red.

La mensajería instantánea también está considerada dentro de este apartado, así como la inclusión de acuerdos de confidencialidad y, por su puesto, de no divulgación respecto a la información a la que tienen accesos los colaboradores de la organización.

A.14: Adquisición, desarrollo y mantenimiento de Sistemas: apartado que establece los controles que se pueden aplicar al ciclo de vida de contratación, desarrollo y mantenimiento de aplicaciones y software, ya sea que se trate de una fábrica de desarrollo interna o externa a la organización.

Los controles están orientados a proteger los datos e información que se pueden utilizar como insumos dentro del proceso de desarrollo de información, disminuyendo el riesgo que implica la réplica de dicha información desde ambientes productivos hacia ambientes no productivos.

A.15: Relaciones con los proveedores: esta sección brinda una guía exclusiva para asegurar los procesos y actividades que se desarrollan fruto de la contratación de proveedores. Busca normar y formalizar por escrito aquellas atribuciones que se pueden asignar al proveedor y su equipo de trabajo, de tal forma que se eviten acciones o comportamientos que pongan en riesgo la información de la organización.

A.16: Gestión de Incidentes en Seguridad de la Información: considerando que al día hoy es prácticamente inevitable que se presenten

incidentes relacionados son la seguridad de la información, esta sección aporta controles que permitan una adecuada gestión de dichos eventos.

Entre dichos controles se incluyen la designación de responsabilidades, reporte de eventos, identificación y reporte de debilidades, respuesta ante los eventos, recolección de evidencia, aprendizaje a partir de los incidentes, entre otros.

A.17: Continuidad del Negocio: este apartado se enfoca en proveer controles que permitan asegurar la continuidad del negocio en caso de eventos catastróficos que pudieran afectar la infraestructura y los activos de información. Estos eventos pueden tener un origen natural, como inundaciones, terremotos y otros, al igual que podría tratarse de eventos provocados, como incendios, actos de vandalismo, entre otros.

A.18: Cumplimiento: esta sección provee controles que busca asegurar que las normas, políticas, obligaciones contractuales y leyes, vigentes, aplicables y referentes a la seguridad de la información, se cumplan de forma satisfactoria, evitando que se incurra en alguna falta que pueda ser sancionable o que pueda acarrear problemas con los clientes de la organización.

2.4. Metodología de análisis y gestión de riesgos

En la sección 1.6 de capítulo 1 se hace un breve acercamiento a la metodología de análisis y gestión de riesgos que será utilizada para el desarrollo del presente trabajo.

La propia norma ISO 27000 presenta, entre sus componentes, el detalle de una metodología compuesta por fases sucesivas que se ejecutan de manera sistemática, de tal forma que cada una de las fases desarrollen, como salida, un entregable que servirá como insumo de entrada para la fase siguiente [19].

Como parte de dicha metodología, se inicia con el análisis de la situación actual de la organización y la respectiva identificación de los activos de información de la organización. A continuación, se ejecuta la categorización y valoración de dichos activos, así como la identificación de los riegos y amenazas que se relacionan a éstos.

Posteriormente se debe ejecutar un análisis y consecuentemente una valoración respecto a los riesgos y amenazas identificadas para, finalmente, proceder con la documentación del esquema de seguridad de la información propuesto en el presente trabajo.

Para valorar las amenazas identificadas, respecto a la seguridad de la información, es preciso determinar la frecuencia o probabilidad de que esta

se presente o suceda, esto puede lograrse estableciendo una escala numérica asignada de acuerdo a la frecuencia, como se detalla a continuación:

1. **Probabilidad mínima o muy baja (Valor 1)**
    a. Hasta el momento no se ha logrado identificar la existencia de posibles entes vulneradores o incidentes que hayan podido suceder con anterioridad. El evento podría suscitarse al menos una vez cada 5 años.
2. **Probabilidad potencial o baja (Valor 2)**
    a. Existen evidencias sobre la existencia de esta categoría de incidentes dentro del nicho de mercado de la organización y/o la zona geográfica en la que esta desarrolla sus actividades, sin embargo, no existe registros de dichos incidentes dentro de la organización. Se puede esperar la ocurrencia esporádica de este tipo de incidentes. El evento podría suscitarse al menos una vez cada 2 años.
3. **Probabilidad creíble o media (Valor 3)**
    a. Existe evidencia de la existencia de esta clase de incidentes dentro de la organización y se espera que este tipo de eventos se presenten periódicamente, sin embargo, no se conoce la frecuencia con la que podrían ocurrir. El evento podría suscitarse al menos una vez cada año.

4. **Probabilidad definida o alta (Valor 4)**
    a. Existe evidencia de la existencia de esta clase de incidentes dentro de la organización y se conoce el origen de las mismas. Este tipo de eventos se presentan con una frecuencia que ya es conocida internamente. El evento podría suscitarse al menos una vez cada 6 meses.

Adicionalmente, es preciso determinar el nivel de vulnerabilidad que representa cada una de las amenazas o, en otras palabras, determinar el impacto potencial que implicaría la materialización de dicha amenaza. La finalidad es conocer cuál es el nivel de afectación que, un incidente relacionado con esta vulnerabilidad, podría causar sobre la operación normal de la organización. Para esto se utiliza una escala numérica que se detalla a continuación:

1. **Menor deterioro o inexistencia del mismo (Valor 1)**
    a. No se evidencia la existencia de impacto en las operaciones de la organización ni en su infraestructura. Si el evento llegara a materializarse, el efecto resultante sería de bajo impacto sobre la organización.
2. **Perceptible o deterioro bajo (Valor 2)**
    a. Si el evento llegara a materializarse, el efecto resultante sería de medianas consecuencias sobre la organización. La mayor parte

de la infraestructura no se verá afectada, sin embargo, se evidencian daños limitados sobre los activos de información.

3. **Grave o deterioro medio (Valor 3)**
   a. Se evidencia la existencia de ciertos activos de información dañados, al punto de que no podrán ser recuperados, pero la mayoría permanecen sin afectaciones. Si el evento llegara a materializarse, el efecto resultante sería de altas consecuencias sobre la organización.
4. **Catastrófica o deterioro muy grave (Valor 4)**
   a. Si el evento llegara a materializarse, el efecto resultante sería de consecuencias catastróficas sobre la organización. Se producen daños que resultan en la pérdida completa de los activos, datos e información, lo que imposibilita alguna restauración o reparación de los mismos.

2.5. Actualidad respecto a los ataques informáticos

Referente a la actualidad relacionada con las estadísticas de los ataques informáticos y el nivel de preparación para prevenirlos, reportados por organizaciones alrededor del mundo, la International Telecommunication Union (ITU) presenta periódicamente un estudio con el respectivo detalle.

Entre los componentes del estudio, previamente mencionado, se detalla una encuesta que combina 25 indicadores medidos en los 193 países miembros de las ITU. Estos 25 indicadores hacen referencia a los 5 pilares fundamentales de la ciberseguridad, según ITU: los aspectos legales, los aspectos técnicos, los aspectos organizacionales, el desarrollo de capacidades y los niveles de cooperación [20].

Como resultado del último estudio realizado, en el año 2018, se determinó que el top de los países que mejores resultados obtuvieron, en cada uno de los índices analizados, está encabezado por Reino Unido, Estados Unidos y Francia. Por otro lado, Ecuador se ubica en la posición 98, Perú en la 95 y Colombia en la 73 [20].

Rank	Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
2	United States of America	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.193	0.200	0.186	0.139
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.192	0.195	0.125
7	Spain	0.896	0.200	0.180	0.200	0.168	0.148
8	Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
9	Norway	0.892	0.191	0.196	0.177	0.185	0.143
10	Canada	0.892	0.195	0.189	0.200	0.172	0.137
11	Australia	0.890	0.200	0.174	0.200	0.176	0.139

Figura 2.7 Países más comprometidos con la ciberseguridad [20].

Por otra parte, a nivel interno, el Ministerio de Telecomunicaciones reportó que, durante el año 2019, a partir del retiro del asilo político que se había concedido a Julian Assagne, el país pasó de experimentar un promedio de 20 millones de ataques a experimentar más de 40 millones de ataques, la intensidad fue tal que, el día sábado 11 de abril de 2019, de escaló de la posición 51 a la posición 31 en la escala mundial referente a ataques informáticos [21].

Complementariamente, ESET brinda una lista de los principales malware que han sido detectados durante el tercer trimestre de 2020, misma que está encabezada por Troyano VBA, Troyano LNK y Troyano Win [22].

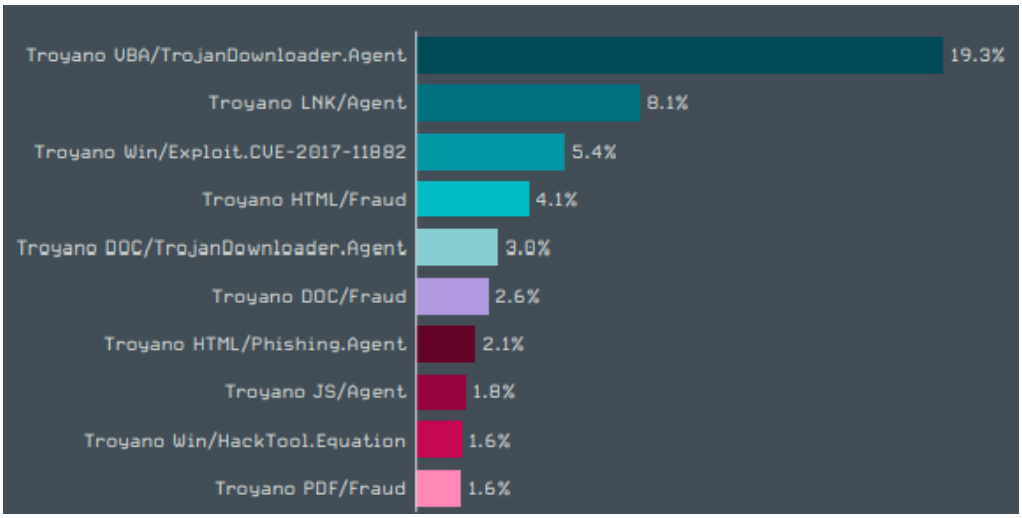


Figura 2.8 Detecciones de malware Q3 2020 a nivel global [*22*]

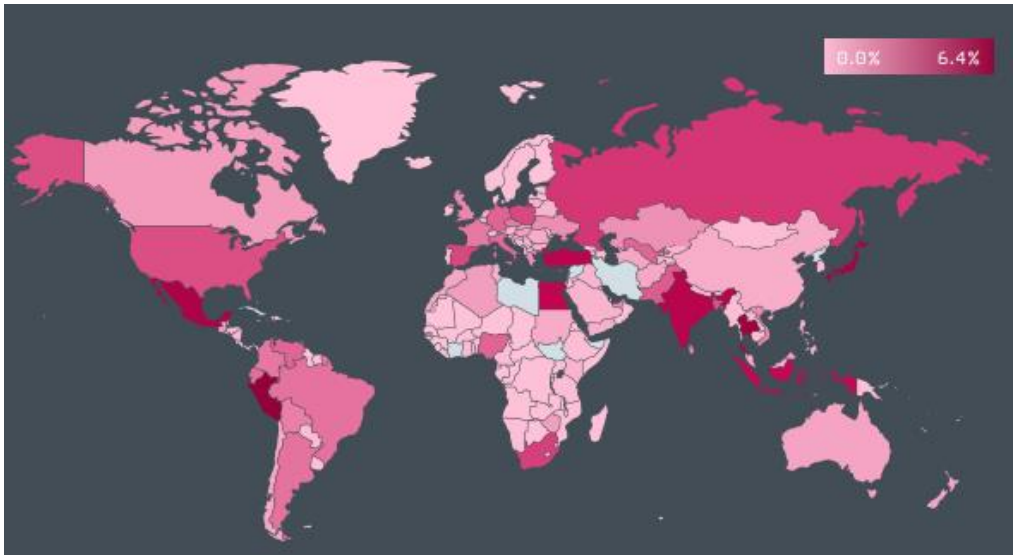


Figura 2.9 Mapa de calor en detección de malware Q3 de 2020 [22]

Por su parte, Kaspersky reporta que, en Ecuador durante el periodo comprendido entre el 21 de enero y el 26 de enero de 2021, se detectó un pico de 1’174.795 intentos de intrusión (Figura 2.11), de los cuales un 76% corresponden al agente “Intrusion.Win.MS17-010.o” y un 17% al agente “Bruteforce.Generic.Rdp/” (Figura 2.12) [23]

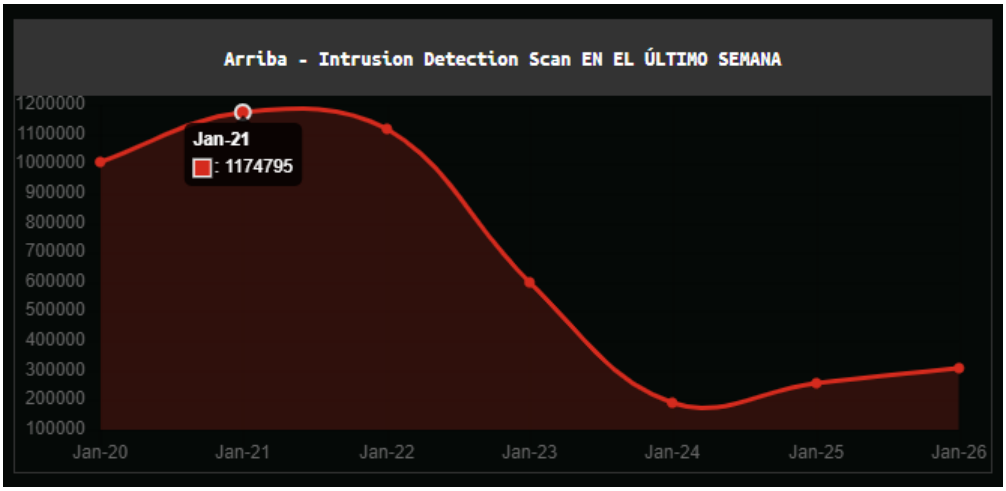


Figura 2.10 Intentos de intrusión en Ecuador [*23*]

Arriba - Intrusion Detection Scan EN EL ÚLTIMO SEMANA		
1	Intrusion.Win.MS17-010.o	76.71%
2	Bruteforce.Generic.Rdp.d	17.36%
3	Scan.Generic.PortScan.TCP	2.38%
4	Intrusion.Win.MS17-010.p	2.1%
5	Bruteforce.Generic.Rdp.a	0.98%
6	DoS.Generic.Flood.TCPSYN	0.2%
7	Intrusion.Win.MS17-010.cf	0.15%
8	Scan.Generic.PortScan.UDP	0.05%
9	Intrusion.Generic.CVE-2018-1273.exploit	0.01%
10	Intrusion.Win.IIS.UNICODE.a.exploit	0.01%

Figura 2.11 Agentes intrusivos en Ecuador [23]

CAPÍTULO 3

3. SEGURIDAD DE LA INFORMACIÓN EN NEGYSERT

3.1. Análisis de la situación actual

La directiva de Negysert S.A., considerando lo reñido y competitivo del mercado de los servicios de TI y con miras a establecer una nueva línea de negocios como objetivo estratégico de la organización, ha decidido enfocar parte de sus esfuerzos en diferenciase de la competencia, a través del mejoramiento de su imagen corporativa.

Como parte de esa diferenciación, se ha decidido trabajar en el desarrollo de una primera versión, o versión base, de un esquema de seguridad de la información basado en ISO/IEC 27001. Mismo que se establecerá para uno de los procesos operativos y que, posteriormente y de forma independiente, se expandirá en detalle con la intención de conseguir la certificación formal y tener un modelo a replicar que se pueda aplicar a los procesos que se considere pertinente.

Negysert S.A. siendo una PYME de TI, ha dividido su operación en 3 áreas fundamentales, Operaciones, Comercial y Administración & Finanzas, mismas que soportan el desarrollo de sus actividades empresariales.

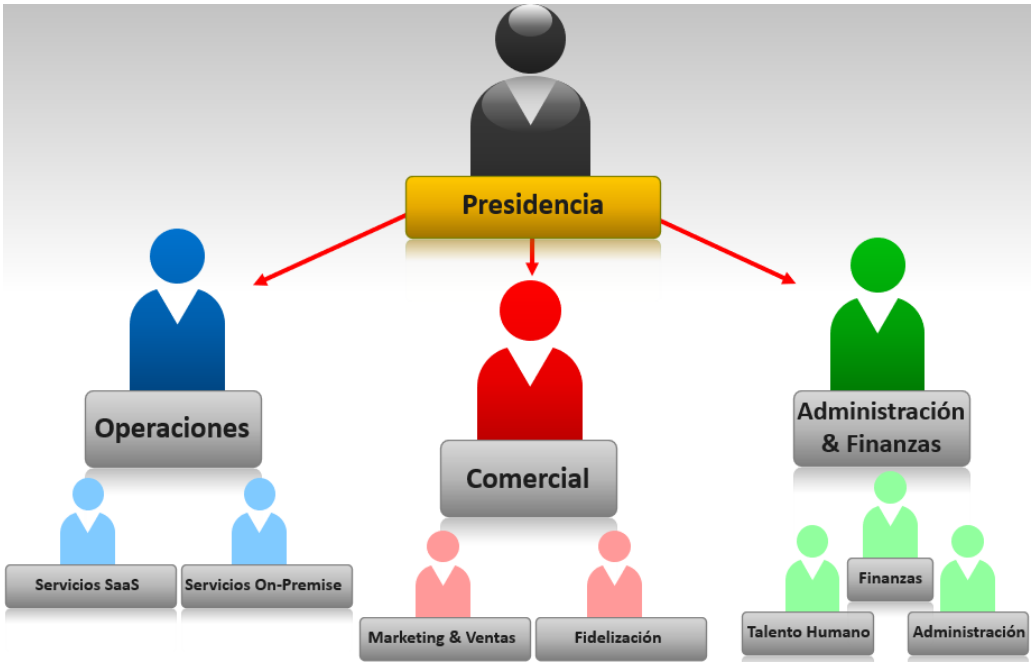


Figura 3.1 Organigrama general Negysert S.A.
Fuente: Autor

Los departamentos de servicios SaaS y On-Premise son los encargados de ejecutar todas las actividades de soporte y monitoreo, relacionados con las 2 principales líneas de negocio que la empresa actualmente maneja, siendo la más importante de ellas la línea de prestación de software como un servicio (SaaS). Estás 2 líneas de negocio se apoyan sobre un sistema ERP, que ha sido desarrollado y madurado por la empresa desde los inicios de ésta.

Inicialmente, el sistema se desarrolló bajo el nombre de “Semiya Software” y su principal modelo comercial consistía en implementaciones On-Premise. Con el transcurso del tiempo y el cambio de las tendencias en el mercado, el ERP fue rebautizado bajo el nombre de “Titanium Software” y su modelo de negocio tomó un mayor énfasis hacia la figura de SaaS, software como un servicio.

Paralelamente, las áreas de servicios SaaS y On-Premise están brindando el soporte necesario para la incursión en una línea de negocios emergente, la recolección de datos, análisis y generación de estadísticas, misma que se ha determinado como parte de los objetivos estratégicos de la empresa.

A continuación, la figura 3.2 brinda una visión macro de los procesos que soportan la operación de Negysert S.A.:

Figura 3.2 Mapa macro de procesos Negysert S.A.
Fuente: Autor

3.2. Identificación y análisis de los involucrados y/o interesados

Con la finalidad de conseguir un esquema de seguridad de la información lo más ajustado a la realidad y el entorno de Negysert, se realiza la identificación y análisis de los interesados e involucrados en la operación de la compañía, determinando como los de mayor importancia o influencia a los siguientes:

1. **Clientes**

- **Requisitos**

i. Recibir servicios que logren su satisfacción.

ii. Evitar afectaciones a su información.

- **Expectativas**
    i. Mejorar las capacidades actuales de la organización respecto a la satisfacción del cliente.
    ii. Implementar los controles que aseguren los 3 pilares fundamentales de la información, para el cliente.

2. Proveedores

- **Requisitos**
    i. Mantener niveles de cooperación mutuamente beneficiosos.
    ii. Compartir información relevante para la relación comercial.
    iii. Evitar tratamiento inadecuado a los recursos compartidos.
- **Expectativas**
    i. Garantizar que la información compartida con los proveedores se maneje de forma que se mantengan los criterios de confidencialidad, integridad, así como disponibilidad.
    ii. Incentivar al cumplimiento de los acuerdos y políticas de tratamiento de la información compartida.

3. Colaboradores

- **Requisitos**
    i. Contar con el adecuado acompañamiento, procurando asegurar el éxito de la implementación del esquema de seguridad de la información.

ii. Contribuir activamente en la prevención de cualquier situación que ponga en riesgo los 3 pilares fundamentales de la información.

iii. Socializar todas las acciones que se tomen como parte del establecimiento del esquema de seguridad de la información.

- **Expectativas**

i. Conseguir que los colaboradores interioricen la aplicación de buenas prácticas, enfocadas en el aseguramiento de los 3 pilares fundamentales de la información.

ii. Incentivar el cumplimiento de las políticas establecidas.

iii. Incentivar la propuesta de mejoras sobre las políticas y controles establecidos, procurando la mejora continua del esquema de seguridad de la información.

4. Gerencia

- **Requisitos**

i. Proporcionar el apoyo necesario para el desarrollo e implementación del esquema de seguridad de la información.

ii. Asignar los recursos necesarios para el desarrollo e implementación del esquema de seguridad de la información.

iii. Participar activamente en la definición del tratamiento que se dará a los riegos, especialmente de aquellos que se aceptarán

- **Expectativas**
    i. Que el esquema de seguridad, que se defina, esté alineado con los objetivos estratégicos de la organización.
    ii. Que los colaboradores demuestren su predisposición para contribuir con el esquema de seguridad de la información.
    iii. Que el esquema de seguridad a definir sirva como plantilla para realizar la implementación sobre otros procesos de la organización

3.3. Análisis de brechas

Con la finalidad de determinar el estado actual de la organización, respecto a los controles, políticas y procedimientos relacionados con la seguridad de la información, se efectúa un “Análisis de Gap o Análisis de Brecha”. Entendiendo que el término “GAP” hace referencia a el punto en el que se encuentra la organización actualmente (presente) y el punto donde la organización quiere estar o lo que quiere lograr (futuro).

Este análisis permite identificar lo que a la organización le hace falta o los puntos en los que debe enfocar sus esfuerzos, así como los recursos que deberá asignar para la consecución exitosa de los objetivos planteados o metas. En otras palabras, puede considerarse que este análisis representa

una auditoría inicial que evidenciará el grado de cumplimiento o implementación de la norma ISO/IEC 27001 en la organización.

Para la ejecución del análisis, y por recomendación de la propia norma, se trabajará considerando niveles de madurez respecto al cumplimiento de los controles sugeridos por la norma. Los niveles de madurez a considerar se trabajarán en base a CMM y se describen a continuación [24]:

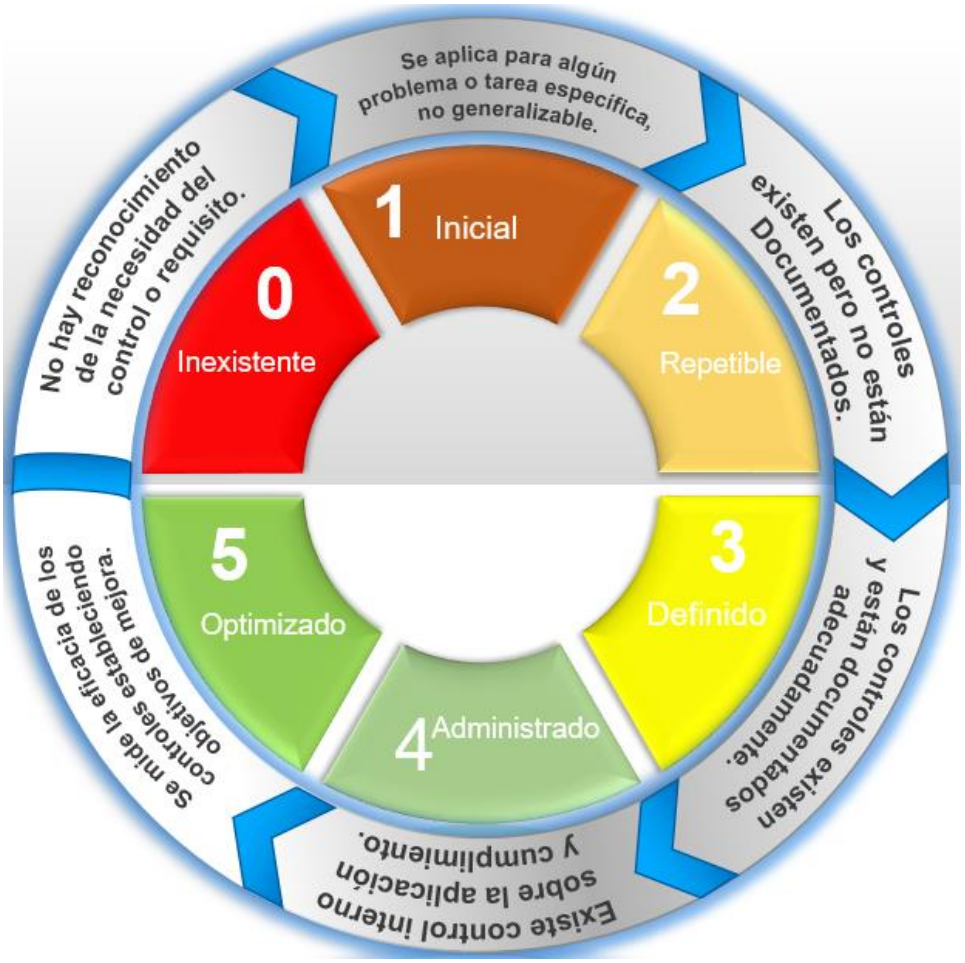


Figura 3.3 Niveles de madurez.
Fuente: Autor

Los niveles de madurez, anteriormente descritos, se utilizan para calificar el nivel de cumplimiento que actualmente mantiene la organización respecto a los controles sugeridos por la norma. Para este cometido, se ha desarrollado un cuestionario, detallado en el Anexo A, mismo que se ha aplicado a la organización.

Considerando que Negysert S.A. es una empresa pequeña, la aplicación del cuestionario se trabajó en una sola sesión y se contó con la participación de los siguientes integrantes de la organización:

- Ing. José Luis Paredes – Gerente General
- Ing. Rogger Cedeño – Jefe de Operaciones
- Ing. Luis Ortega – Jefe de Administración y Finanzas

3.4. Resultados del análisis de brechas

Para la obtención de calificaciones promedio del nivel de madurez, para cada uno de los apartados de la norma, se realizó la suma de la calificación individual de cada ítem de control y este valor se lo dividió para la cantidad de ítems de control del apartado, de acuerdo a la siguiente formula:

$$Nivel\ promedio = \frac{Suma\ de\ la\ calificación\ de\ cada\ ítem\ de\ control}{Cantidad\ de\ ítems\ de\ control}$$

Estos valores promediados permiten determinar el nivel de madurez de acuerdo a la siguiente tabla:

NIVEL	MADUREZ
< 1	Inexistente
< 2	Inicial
< 3	Repetible
< 4	Definido
< 5	Administrado
5	Optimizado

Tabla 1 Niveles promedio de madurez
Fuente: Autor

A continuación, en la tabla 3.2, se presenta el resumen de los resultados obtenidos a partir de la aplicación del cuestionario de cumplimiento sobre los controles de la norma:

Cláusula	Anexo A ISO 27001	Puntaje	Nivel
A5	Políticas de Seguridad de la Información	0.00	Inexistente
A6	Organización de la Seguridad de la Información	0.00	Inexistente
A7	Seguridad en los Recursos Humanos	0.67	Inexistente
A8	Gestión de Activos	0.50	Inexistente
A9	Control de Acceso	0.45	Inexistente
A10	Criptografía	0.00	Inexistente
A11	Seguridad Física y del entorno	0.67	Inexistente
A12	Seguridad en las Operaciones	1.19	Inicial
A13	Seguridad en las Comunicaciones	1.00	Inicial

Cláusula	Anexo A ISO 27001	Puntaje	Nivel
A14	Adquisición, desarrollo y mantenimiento de sistemas de información	1.85	Inicial
A15	Relación con Proveedores	1.33	Inicial
A16	Gestión de incidentes de seguridad de la información	0.57	Inexistente
A17	Gestión de la Continuidad del Negocio	0.00	Inexistente
A18	Cumplimiento Legal y Contractual	0.40	Inexistente
	Cumplimiento Promedio General	**0.62**	**Inexistente**

Tabla 2 Nivel de Cumplimiento Actual
Fuente: Autor

El análisis de brechas ejecutado refleja que Negysert S.A. no ha logrado desarrollar, hasta el momento, un enfoque estructurado y orientado hacia la adopción de las mejores prácticas respecto a lo que a seguridad de la información se refiere.

La aplicación del cuestionario, detallado en el Anexo A, refleja que los apartados sobre los que al menos se ha considerado algún control, respecto a la norma ISO/IEC 27001, alcanzan apenas un nivel de madurez “INICIAL”. Siendo, de éstos, el apartado mejor calificado el que hace referencia a la “adquisición, desarrollo y mantenimiento de sistemas de información”, con un puntaje promedio de 1.85, seguido de los apartados de “relación con proveedores”, “seguridad en las operaciones” y “seguridad en las comunicaciones” con puntajes de 1.33, 1.19 y 1.00 respectivamente.

CAPÍTULO 4

4. DISEÑO DEL ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN

4.1. Identificación de los activos de información de la empresa

Para el desarrollo del esquema de seguridad de la información, propuesto como parte medular del presente trabajo, la directiva de la organización ha decidido enfocar este primer esfuerzo en el proceso denominado como “Administración de Servicios SaaS”. De esta forma, y una vez completamente pulido el esquema de seguridad de la información, podrán continuar con la inclusión de los procesos restantes, utilizando como guía el trabajo aquí realizado.

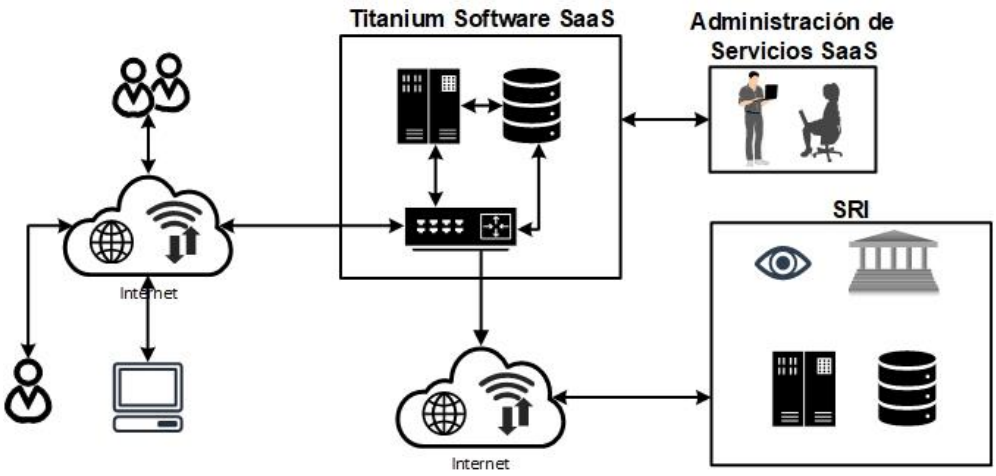


Figura 4.1 Arquitectura de alto nivel del proceso de "Administración de Servicios SaaS"
Fuente: Autor

El proceso de “Administración de Servicios SaaS” tiene como objetivo asegurar la disponibilidad del servicio de “Titanium Software”. Para este cometido, se cuenta con un equipo administración de servicios, mismo que se encarga de monitorear el correcto funcionamiento e interacción del sistema, tanto con los clientes suscritos como con el ente de control tributario al que se conecta, Servicio de Rentas Internas (SRI).

El desarrollo de las actividades de monitoreo y control se llevan a cabo localmente, a través de una red LAN, mientras las interacciones con los clientes suscritos y con el SRI se realizan a través de internet.

Con base a lo expuesto, se lleva a cabo la identificación de los activos de información que intervienen en el proceso de “Administración de Servicios SaaS”. Para este cometido se utiliza como guía el catálogo de elementos

incluido como parte de la metodología Magerit, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, V3.

Magerit constituye una respuesta a esa creciente e innegable dependencia que la sociedad, y todas sus organizaciones, ha desarrollado y continuará desarrollando respecto a las tecnologías de la información y comunicaciones, cuando se trata de lograr los objetivos trazados. Si bien es evidente que el uso de las TIC genera grandes beneficios, tampoco es desconocido que este uso acarrea sus respectivos riesgos, mismos que se deben administrar de forma prudente mediante la aplicación de las mejores prácticas de la seguridad de la información[25].

Para realizar una correcta identificación de los activos que intervienen en el proceso, de “Administración de Servicios SaaS”, es importante tener en cuenta que estos pueden ser tanto tangibles como intangibles. Por ejemplo, los servicios que son entregados por el proceso, la información que éste procesa, los informes que permite imprimir, el hardware que lo soporte, las personas que intervienen, entre otros[26].

A continuación se definen conceptos de los principales tipos de activos de información que se pueden encontrar como parte del proceso seleccionado[26]:

- **Software**. – hace referencia a las automatizaciones que se han desarrollado por parte de un departamento de software. Estas

pueden recibir diversas denominaciones, como, por ejemplo: desarrollos, aplicativos, programas, aplicaciones, sistema gestor de base de datos, ERPs, etc.

- **Hardware**. – se define como el equipamiento o medios físicos que brindan soporte, ya sea de forma directa o indirecta, a los servicios desplegados por la organización. Entre ellos podemos mencionar: servidores, dispositivos periféricos, dispositivos de redes, computadores personales, dispositivos de telefonía, etc.
- **Personal**. – refiere a las personas que interactúan o están relacionadas con los activos de información de la organización. Entre estos se pueden mencionar a: usuarios internos y externos, administradores de sistemas y plataformas, proveedores y personal subcontratado.
- **Información.** – considerada actualmente como uno de los activos más importantes en las organizaciones, pues soportan la prestación de los servicios que estas ofertan. Este activo puede presentarse de dos formas:
    - **Digital**. – como en ficheros digitales, bases de datos, respaldos digitales, imágenes, entre otros. Con su principal característica de presentarse en formato electrónico.
    - **Física**. – manuales impresos de políticas, reglamentos, bitácoras, procedimientos, reportería generada de los

sistemas, entre otros. Con su principal característica de presentarse en formato físico, a través de algún tipo de impresión.

- **Instalaciones**. – hace referencia exclusivamente a la infraestructura que hospeda a los equipos informáticos, sistemas de información y equipos de telecomunicaciones. Por ejemplo: edificios, oficinas, instalaciones de respaldo, plataformas móviles (vehículos terrestres, marítimos y aéreos).
- **Servicios**. – refiere a los servicios prestados por los sistemas informáticos, sean estos internos o externos, y que tienen la finalidad de satisfacer las necesidades de los usuarios. Entre ellos podemos nombrar a: servicios de correo, servicios de almacenaje de datos, servicios de acceso a internet, entre otros.
- **Comunicaciones**. – hace referencia tanto a las instalaciones propias de la organización como a servicios que se hayan podido contratar a terceros y que son utilizados para transportar o transferir datos desde un punto de origen a un punto de destino.

A continuación se definen conceptos de los principales tipos de activos de información que se pueden encontrar como parte del proceso seleccionado[26]:

Sigla	Tipo de Activo	Total
CO	Comunicaciones	6
HW	Hardware	8
IF	Información	10
IN	Instalaciones	2
OT	Otros	1
PE	Personal	3
SE	Servicio	2
SW	Software	7
Total Activos		**39**

Tabla 3 Resumen de activos de información del proceso "Administración de Servicios SaaS"
Fuente: Autor

El detalle de los activos de la información, relacionados con el proceso de "Administración de Servicios SaaS", podrá ser revisado en el “Anexo B”, al final de este documento.

4.2. Categorización de los activos de información, del proceso “Administración de Servicios SaaS”, según criticidad

Para realizar asegurar un adecuado enfoque de los recursos, a la hora de establecer los controles que se deben aplicar como parte del esquema de seguridad de la información, es preciso que los activos de información

sean categorizados, de acuerdo al grado de criticidad que cada uno de ellos posea como parte de la operación del proceso de “Administración de Servicios SaaS.

En este sentido, ISO 27001:2013 no impone ninguna escala en cuanto en a la valoración de la criticidad de los activos de información. Sin embargo, para llevar a cabo la valoración en mención, se ha establecido una escala de seis valores para calificar los tres criterios básicos respecto a la información (integridad, confidencialidad y disponibilidad). El promedio que se obtenga, a partir de las calificaciones de los tres criterios, permitirá asignar una escala de importancia del activo de información calificado.

A continuación, se detalla la escala de valores a utilizar como parte de la categorización de los activos de información.

Confidencialidad		**Disponibilidad**		**Integridad**		**Importancia**	
0	No Aplica	0	No Aplica	0	No Aplica	0	No Aplica
1	Pública	1	Muy Baja	1	Muy Baja	1	Muy Baja
2	Uso Interno	2	Baja	2	Baja	2	Baja
3	Restringida	3	Media	3	Media	3	Media
4	Confidencial	4	Alta	4	Alta	4	Alta
5	Secreta	5	Crítica	5	Crítica	5	Crítica

Tabla 4 Escala de valoración, de acuerdo a los criterios, de activos de información del proceso "Administración de Servicios SaaS"
Fuente: Autor

Valoración Cuantitativa	Valoración Cualitativa	Descripción
0	No Aplica	El criterio de importancia no aplica para el activo de información.
1	Muy Baja	El activo no afecta procesos.
2	Baja	El activo podría afectar una tarea aislada de la operación o del proceso. Las pérdidas o afectación serían menores y no incurrirían en sanciones pecuniarias.
3	Media	El activo puede afectar de forma parcial una operación o un proceso. Las pérdidas o afectaciones podrían ser moderadas.
4	Alta	Uno o varios procesos pueden ser seriamente afectados. Las pérdidas o afectaciones podrían causar sanciones.
5	Crítica	La organización podría verse seriamente afectada, tanto por la generación de sanciones elevadas como por la reducción de la credibilidad de la organización y sus procesos.

Tabla 5 Escala de criticidad o importancia de los activos de información del proceso "Administración de Servicios SaaS"
Fuente: Autor

El detalle de la categorización de los activos de información, del proceso "Administración de Servicios SaaS", puede ser revisado en el “Anexo C”.

4.3. Identificación de las amenazas

Una vez realizado el inventario de activos de información del proceso de "Administración de Servicios SaaS", y con la debida valoración de acuerdo a las 3 dimensiones más importantes de estos, el siguiente paso consiste en la identificación de las amenazas a las que dichos activos se encuentran expuestos.

Si bien el establecimiento de un esquema de seguridad de la información, basado en ISO 27001:2013, es un proceso compuesto por varias etapas que cuentan con su respectivo nivel de importancia para dicho cometido; el proceso o la etapa de identificación de las amenazas bien puede considerarse como una de las más importantes. Este proceso permite tener claridad sobre aquellos eventos de los que hay que proteger los activos de información, así como de las posibles estrategias que podrían implementarse para conseguirlo.

Alineados con la metodología Magerit V3[25], para la identificación de las amenazas se considera la siguiente tipificación:

- **De origen natural**. – aquellos eventos que obedecen exclusivamente a todo tipo de accidentes naturales, como podrían ser las inundaciones y los terremotos, por ejemplo. En estos escenarios, el activo de información se considera como una víctima pasiva, sin embargo, es importante evaluar la repercusión que se podría tener.
- **Del entorno**. – refiere a aquellos eventos que podrían suscitarse en el entorno directo en el que el activo de información desarrolla su operación y que son ajenos al origen natural; por ejemplo, la posibilidad de algún fallo en la red eléctrica, un fallo estructural en las instalaciones, entre otros.

En estos escenarios, el activo de información se considera una víctima pasiva, pero bien se podrían establecer controles orientados a la prevención.

- **Defectos de las aplicaciones**. – corresponden a las amenazas que se presentan debido a alguna vulnerabilidad propia del activo de información, misma que se origina debido a algún fallo o deficiencia en su diseño; estas vulnerabilidades son regularmente conocidas como vulnerabilidades técnicas.
- **Originadas por las personas de manera accidental**. **–** obedecen a los problemas que podrían originar aquellos usuarios que tienen acceso directo a los activos de información, mismos que pueden ser errores u omisiones. Este tipo de amenazas se incrementa cuando no se segregan de forma correcta los privilegios y accesos que se asignan a los usuarios, de acuerdo a las necesidades de sus funciones.
- **Originadas por las personas de manera deliberada**. – en el mismo sentido que las amenazas originadas de manera accidental, las originadas de manera deliberada se ven drásticamente incrementadas por el exceso de accesos a los activos de información. En esta categoría se habla ya de ataques intencionados que se originan con la finalidad de obtener algún

beneficio o simplemente de perjudicar al propietario de los activos de información.

Cabe resaltar que no todos los tipos de amenazas, ni todas las amenazas, tienen la capacidad de afectar a todo el inventario de activos de información de la organización.

Para identificar las amenazas a las que se encuentran expuestos los activos de información, del proceso de "Administración de Servicios SaaS", se desarrollaron mesas de trabajo con el equipo de Operaciones de Negysert S.A. Como resultados de dichas reuniones se pudo levantar la información detallada en el “Anexo D” del presente documento.

4.4. Análisis y valoración de los riesgos

Con base en lo descrito en el apartado 2.4 de este documento, Metodología de análisis y gestión de riesgos; a continuación, se presentan las escalas de valoraciones cualitativas y cuantitativas utilizadas para la evaluación de los riesgos:

Probabilidad de ocurrencia		
Valoración Cuantitativa	**Valoración Cualitativa**	**Descripción**
1	Muy Baja	El evento podría suscitarse al menos una vez cada 5 años.
2	Baja	El evento podría suscitarse al menos una vez cada 2 años.
3	Media	El evento podría suscitarse al menos una vez cada año.
4	Alta	El evento podría suscitarse al menos una vez cada 6 meses.

Tabla 6 Escala de probabilidad de ocurrencia
Fuente: Autor

Impacto potencial		
Valoración Cuantitativa	**Valoración Cualitativa**	**Descripción**
1	Menor	Si el evento llegara a materializarse, el efecto resultante sería de bajo impacto sobre la organización.
2	Perceptible	Si el evento llegara a materializarse, el efecto resultante sería de medianas consecuencias sobre la organización.
3	Grave	Si el evento llegara a materializarse, el efecto resultante sería de altas consecuencias sobre la organización.
4	Catastrófico	Si el evento llegara a materializarse, el efecto resultante sería de consecuencias catastróficas sobre la organización.

Tabla 7 Escala de impacto potencial
Fuente: Autor

Para obtener o asignar el valor del riego de cada una de las amenazas identificadas y detalladas en el anexo D, se procede a realizar la multiplicación del valor cuantitativo de la probabilidad de ocurrencia por valor cuantitativo del impacto potencial. A partir de dichas operaciones, se obtiene la matriz de valoración de riesgos que se detalla gráficamente a continuación:

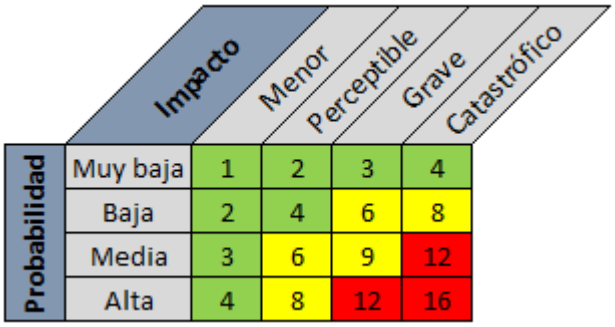


Tabla 8 Matriz de Riegos
Fuente: Autor

Una vez aplicada la matriz de valoración de riesgos, sobre el anexo de Identificación de las Amenazas, Anexo D, se obtienes la matriz de Análisis y Valoración de los Riesgos o Anexo E. En este anexo se detalla cada una de las amenazas identificadas con su respectiva calificación de riesgo.

A continuación, se muestran de forma resumida los riesgos identificados de acuerdo a cada tipo de activo:

	Riesgo			
Tipo Activo	**Aceptable**	**Medio**	**Alto**	**Total**
Comunicaciones	37	35	0	72
Hardware	45	26	6	77
Información	108	60	2	170
Instalaciones	3	0	0	3
Personal	12	12	0	24
Servicios	9	3	0	12
Software	62	22	0	84
Total	276	158	8	442

Tabla 9 Resumen de riegos
Fuente: Autor

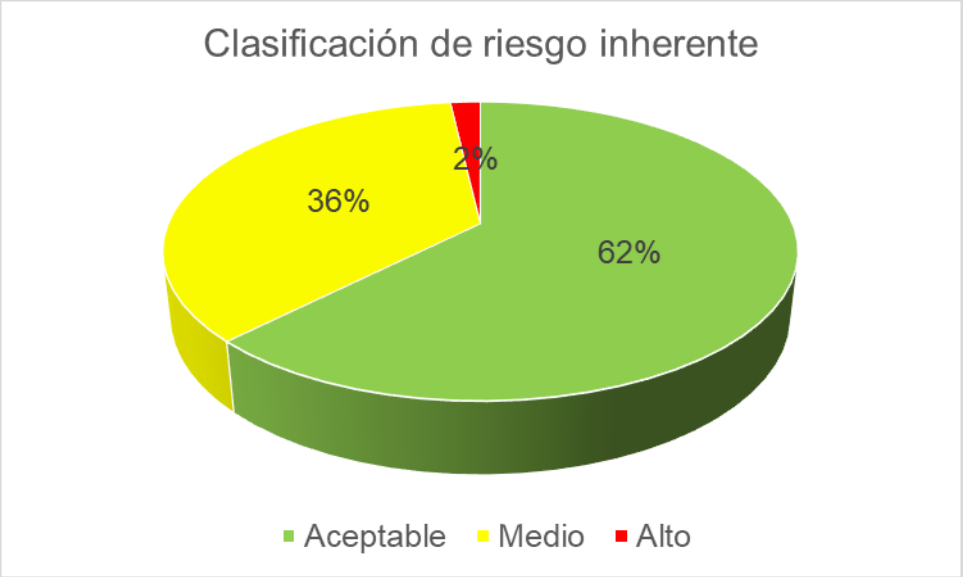


Figura 4.2 Clasificación de riesgo inherente
Fuente: Autor

4.5. Tratamiento de los riesgos

Habiendo realizado el levantamiento pertinente respecto al inventario de activos, al inventario de amenazas y las respectivas valoraciones que corresponde; alineados con la norma ISO 27001:2012, a continuación, se definen las acciones que Negysert S.A. acogerá para el tratamiento de los riegos:

- **Mitigar el riesgo**. – acción que persigue la disminución de los riesgos identificados hasta un nivel que resulte aceptable para la organización, de acuerdo al criterio subjetivo de los involucrados en

el proceso. Para este cometido, se deben implementar los controles que la norma ISO 27001:2013 propone en su Anexo A.

- **Transferir el riesgo**. – la transferencia del riesgo consiste en la contratación o la generación de acuerdos con terceros que se convertirán en responsables del riego, asumiendo cualquier impacto que este genere en caso de materializarse. Un claro y sencillo ejemplo de transferencia de un riesgo consiste en la contratación de una póliza de seguro para un determinado riesgo.
- **Evitar el riesgo**. – si bien no se trata exactamente de una gestión del riesgo como tal, evitar el riesgo consiste en la eliminación de aquello que origina el riesgo. Esto es, por ejemplo, si la incursión en un nuevo nicho de mercado está generando determinado riesgo, revertir dicha incursión evitaría por completo el riego en mención.
- **Aceptar el riesgo**. – este tipo de tratamiento se estila o se aplica normalmente en aquellos riesgos que no tendrían una repercusión importante en el caso de llegar a materializarse o aquellos riegos identificados como “pequeños”. Aceptar el riesgo significa que no se realizará ninguna acción preventiva o no se aplicará ningún control.

4.6. Objetivos del esquema de seguridad de la información

Sabiendo que, como parte de sus objetivos estratégicos, Negysert S.A. busca mejorar o asegurar su proceso de prestación de servicios SaaS y, por otra parte, dar un realce a su imagen comercial; apuntando hacia la incursión en una nueva línea de negocios relacionada con el levantamiento de información y generación de estadísticas. A continuación, se detallan los objetivos planteados para el esquema de seguridad de la información:

- Establecer un primer acercamiento de la empresa con la norma de seguridad de la información ISO 27001:2013; mismo que se pretende mejorar con un proceso de revisión continua y que servirá como guía para la inclusión de los demás procesos de la organización.
- Establecer la planificación de las acciones a ejecutar en el corto, mediano y largo plazo, por parte de Negysert S.A., como parte del aseguramiento del proceso de Administración de Servicios SaaS.
- Establecer lineamientos respecto al proceso de mejora continua que debe aplicarse al esquema de seguridad de la información, con la finalidad de mantenerlo actualizado respecto a la evolución de las posibles amenazas.

4.7. Alcance del esquema de seguridad de la información

De acuerdo a los objetivos estratégicos de Negysert S.A. y los recursos de los que ésta puede disponer para la implementación de esquema de seguridad de la información, se define que el alcance del mencionado esquema se focaliza en el proceso de Administración de Servicios SaaS; mismo que en la actualidad se constituye en el eje central del desarrollo de sus actividades empresariales.

Acorde con la limitación en cuanto a recursos disponibles, el alcance se acota un poco más, enfocándose en las amenazas valoradas a partir de un riesgo medio, desde 9 puntos en delante de acuerdo al Anexo E, que afectan a los activos de información categorizados como críticos, descritos en el Anexo C.

Figura 4.3 Alcance del esquema de seguridad de la información
Fuente: Autor

4.8. Selección de controles, según ISO 27001

De acuerdo con los riesgos que han sido seleccionados para su tratamiento, en el apartado 4.7 Alcance del esquema de seguridad de la información, a continuación, se listan los apartados del Anexo A que se han podido identificar como aplicables:

- A5 políticas de seguridad de la información
- A7 seguridad relativa a los recursos
- A8 gestión de activos
- A9 control de acceso
- A10 criptografía
- A12 seguridad de las operaciones
- A13 seguridad en las comunicaciones
- A14 adquisición, desarrollo y mantenimiento de los sistemas de información
- A18 cumplimiento

De los apartados detallados se ha procedido con la selección de aquellos controles que mejor se ajusten para la mitigación de los riegos seleccionados, el detalle se evidencia en el Anexo F.

CAPÍTULO 5

5. IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN

5.1. Actividades del plan de implementación

Como parte del plan de implementación, del esquema base de seguridad de la información, en el siguiente gráfico se listan de forma macro las actividades que se han identificado como parte del alcance del presente trabajo:

Figura 5.1 Actividades del plan de implementación
Fuente: Autor

Cabe resaltar que las actividades han sido catalogadas de acuerdo al estado de las mismas: por hacer (to do), en proceso (in process) y hechas (done). Las actividades que se listan en el carril de “hechas” han sido desarrolladas como parte del presente trabajo; por otra parte, las actividades listadas en los carriles de “por hacer” y “en proceso” se encuentran bajo la exclusiva responsabilidad de Negysert S.A.

5.2. Cronograma y presupuesto de implementación

De acuerdo al alcance y los objetivos planteados por la organización, Negysert S.A., se ha procedido con el desarrollo del cronograma que detalla las tareas a desarrollar como parte de la implementación del esquema base de seguridad de la información. Considerando que se han asignado 2 recursos con una dedicación del 25% para la ejecución de las tareas descritas en el cronograma, el tiempo que será necesario para la finalización de las mismas es de 290 días laborables, con un presupuesto estimad de USD $6.449°°.

Nombre de tarea	Duración	Comienzo	Fin	Costo
Esquema de seguridad ISO 27001	**290 días**	**lun 26/7/21**	**vie 2/9/22**	**$6.449,00**
Análisis de brechas GAP	12 días	lun 26/7/21	mar 10/8/21	$148,80
Análisis del contexto de la organización	10 días	mié 11/8/21	mar 24/8/21	$124,00
Planificación del Esquema	**68 días**	**mié 25/8/21**	**vie 26/11/21**	**$843,20**
Elaboración de las políticas	40 días	lun 29/11/21	vie 21/1/22	$496,00
Documentación del esquema	**85 días**	**lun 24/1/22**	**vie 20/5/22**	**$1.440,00**
Implementación del esquema	**33 días**	**lun 23/5/22**	**mié 6/7/22**	**$409,20**
Comunicación y sensibilización	10 días	jue 7/7/22	mié 20/7/22	$634,00
Auditoría interna según ISO 27001	12 días	jue 21/7/22	vie 5/8/22	$148,80
Revisión por la dirección según ISO 27001	5 días	lun 8/8/22	vie 12/8/22	$405,00
Proceso de certificación ISO 27001	15 días	lun 15/8/22	vie 2/9/22	$1.800,00

Figura 5.2 Cronograma y presupuesto resumidos
Fuente: Autor

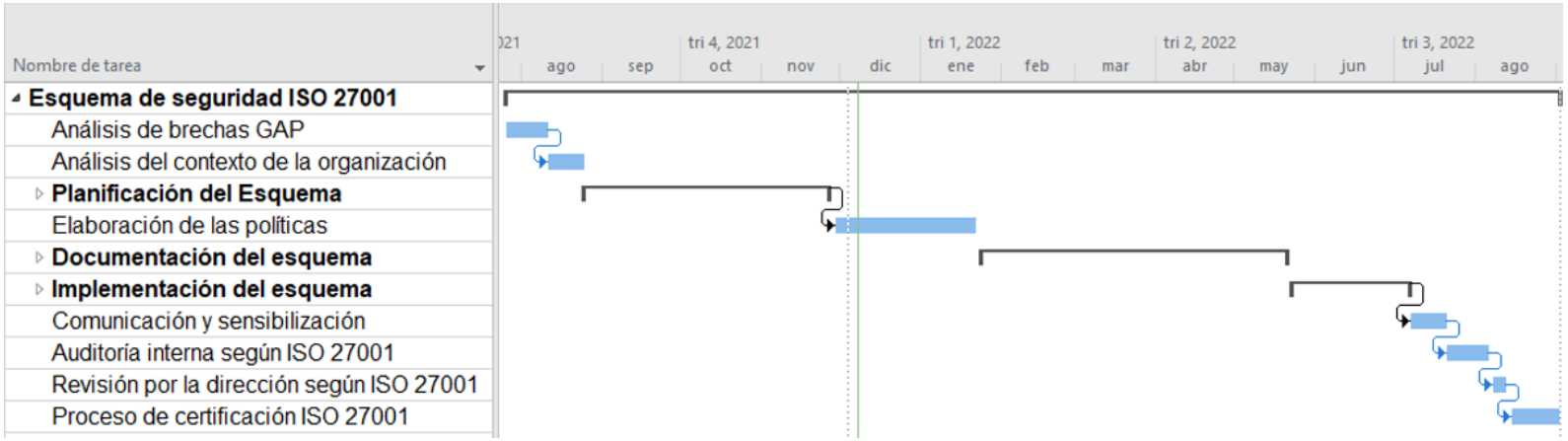


Figura 5.3 Cronograma resumido
Fuente: Autor

Para verificar el detalle de las tareas planificadas, los recursos asignamos y demás detalles relacionados al cronograma del presente trabajo, dirigirse al Anexo G.

5.3. Socialización del esquema

Para que la implementación del esquema base de seguridad de la información, que se ha propuesto en el presente trabajo, tenga una mayor probabilidad de éxito y experimente menor resistencia por parte de los miembros de la organización, es sumamente importante que se lleve a cabo la socialización del mismo.

Para este cometido se llevarán a cabo capacitaciones o charlas virtuales, que serán impartidas por parte de la jefatura del equipo de operaciones, con apoyo de los ingenieros y las demás jefaturas.

Considerando que Negysert S.A. es una empresa es pequeña, las charlas serán impartidas a todos y cada uno de los miembros de la organización, dividiéndolos en 2 grupos.

El contenido que se compartirá estará orientado a formar conciencia respecto a la actualidad mundial en cuanto a la seguridad de la información y los riesgos más comunes que diariamente deben ser sorteados en relación a ésta. Por otra parte, se comunicará a detalle las políticas que están siendo implementadas, así como los beneficios que la implementación de estás traerán para la organización. Complementariamente, se hará énfasis en cómo la implementación de estas políticas de seguridad de la información se alinea con los objetivos estratégicos de la organización.

Una vez ejecutada la socialización del esquema base de seguridad de la información, a nivel interno de la organización, se llevará a cabo una campaña de socialización hacia los clientes de la organización; para ello se preparará una presentación detalla al respecto, misma que será compartida a través de correo electrónico con las compañías clientes de Negysert.

5.4. Impacto esperado a partir de la implementación

A partir de la implementación del esquema base de seguridad de la información, uno de los efectos esperados es la concientización de los miembros internos de la organización, así como de los miembros de las organizaciones cliente, respecto a los grandes riesgos que diariamente ponen atentan contra la seguridad de la información a nivel mundial, tanto a nivel corporativo como a nivel personal.

Una vez ejecutada la socialización del esquema base de seguridad de la información, a nivel interno de la organización, se llevará a cabo una campaña de socialización hacia los clientes de la organización; para ello se preparará una presentación detalla al respecto, misma que será compartida a través de correo electrónico con las compañías clientes de Negysert.

Adicionalmente, se espera que la valoración de los riegos, seleccionados para ser mitigados, pasen de un total de 210 puntos a un total de tan solo 101 puntos; situación que representaría una reducción de 52% de los puntos de riesgo.

En cuanto al cumplimiento de los controles del Anexo A de la norma, a continuación, se detallan los resultados esperados:

Cláusula	ANEXO A ISO 27001	Cumplimiento actual	Cumplimiento esperado
A5	Políticas de Seguridad de la Información	0%	90%
A6	Organización de la Seguridad de la Información	0%	75%
A7	Seguridad en los Recursos Humanos	13%	90%
A8	Gestión de Activos	10%	95%
A9	Control de Acceso	9%	90%
A10	Criptografía	0%	80%
A11	Seguridad Física y del entorno	13%	75%
A12	Seguridad en las Operaciones	24%	95%
A13	Seguridad en las Comunicaciones	20%	85%
A14	Adquisición, desarrollo y mantenimiento de sistemas de información	37%	95%
A15	Relación con Proveedores	27%	80%
A16	Gestión de incidentes de seguridad de la información	11%	90%
A17	Gestión de la Continuidad del Negocio	0%	85%
A18	Cumplimiento Legal y Contractual	8%	90%

Figura 5.4 Cumplimiento actual vs esperado
Fuente: Autor

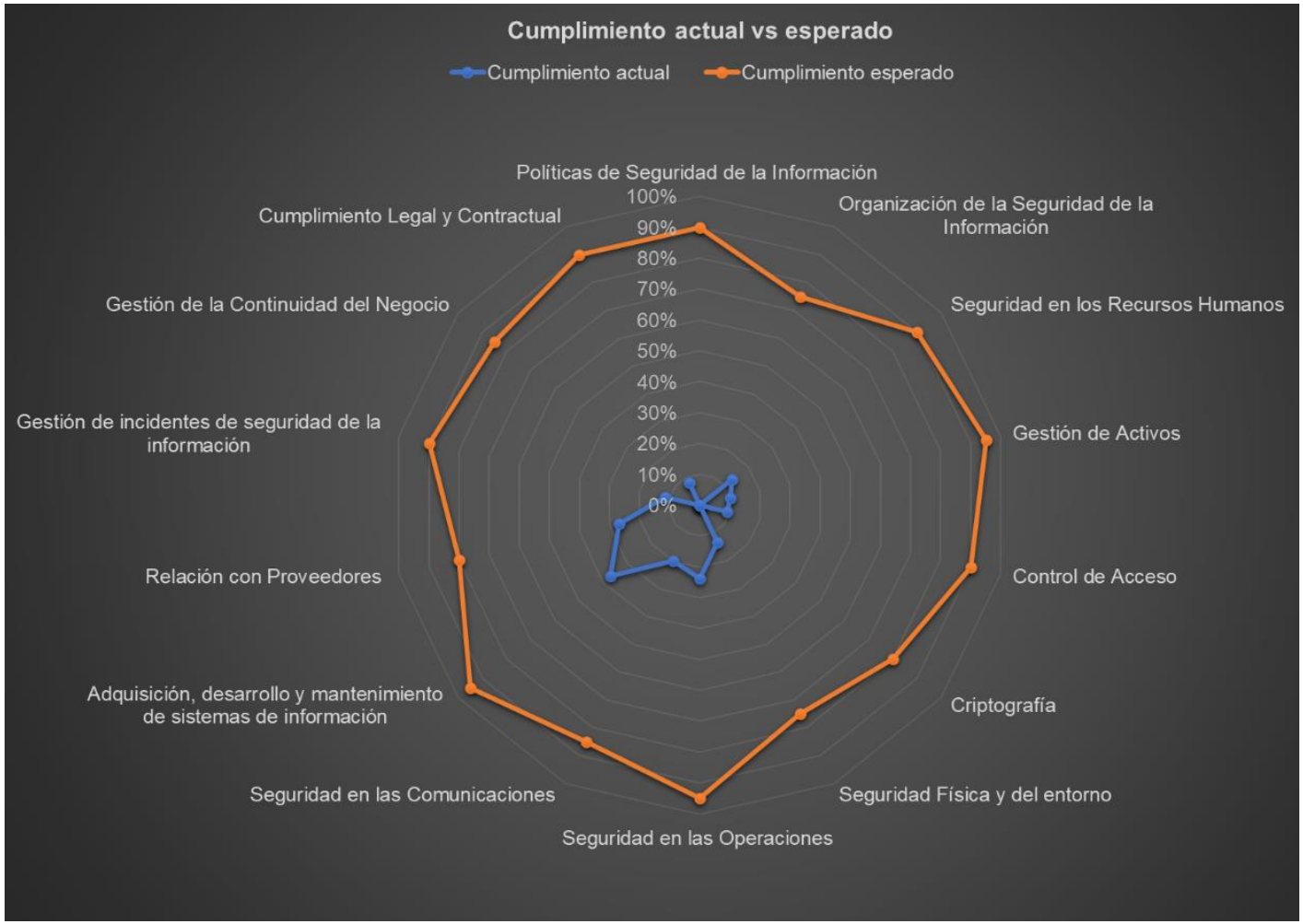


Figura 5.5 Cumplimiento actual vs esperado
Fuente: Autor

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El desarrollo del presente trabajo ha permitido visibilizar que el estado de la empresa respecto a la seguridad de la información, previo al esquema aquí propuesto, realmente se puede considerar como inexistente y que eso se traduce a un cumplimiento nulo y un camino largo por recorrer en cuanto a la norma ISO 27001:2013.

2. Las revisiones estadísticas llevadas a cabo, en cuanto a las ciber amenazas existentes en la actualidad, han evidenciado que el hecho de que Negysert S.A. sea una pequeña empresa no la libera de la posibilidad de sufrir algún ataque en perjuicio de sus activos de información; esto debido a que existe una gama muy diversa motivadores para las personas que se dedican a este tipo de delitos.

3. El levantamiento del inventario de activos de información, pertenecientes al proceso de Administración de Servicios SaaS, ha permitido informar y concientizar a los miembros de la organización sobre elementos que no eran considerados como parte de los activos de información; es decir, se ha comenzado a darle el valor correspondiente a dichos activos.

RECOMENDACIONES

1. Conformar una comisión de seguridad de la información, que debería estar integrada por miembros de la propia organización y de cada una de las áreas. Entre las funciones dicha comisión deberían constar la revisión periódica del cumplimiento adecuado de las políticas de seguridad de la información, así como la catalogación y valoración de los activos de información que puedan ser adquiridos a futuro.

2. Establecer contacto con organizaciones, sean estas estatales o privadas, que tengan un nivel de madurez mayor al de Negysert S.A., en cuanto a seguridad de la información, y compartir información relevante en cuanto a la actualidad y mejores prácticas en dicho campo.

3. Establecer una estrategia que involucre a las empresas clientes de Negysert S.A. y que permita llevar a cabo charlas periódicas, dirigidas hacia el personal de las empresas que formen parte de la alianza. Estas charlas deberían estar enfocadas en la socialización de la actualidad de las amenazas informáticas, así como las mejores prácticas para evitar convertirse en víctimas de éstas.

4. Madurar el esquema de seguridad de la información propuesto, en el contexto del proceso de Administración de Servicios SaaS, para que posteriormente éste pueda ser extendido progresivamente hacia otros procesos de la organización.

BIBLIOGRAFÍA

[1] D. Carvajal, A. Cardona, y F. Valencia, «Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana», *Entre Cienc. e Ing.*, vol. 13, pp. 68-76, 2019.

[2] INEC, «Módulo de TIC de las Encuestas de Manufactura y Minería, Comercio Interno y Servicios», 2015. [En línea]. Disponible en: https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/Tecnologia_Inform_Comun_Empresas-tics/2015/2015_TICEMPRESAS_PRESENTACION.pdf. [Accedido: 26-dic-2020].

[3] INEC, «Encuesta Nacional Multipropósito de Hogares (Seguimiento al Plan Nacional de Desarrollo)», 2018. [En línea]. Disponible en: https://www.ecuadorencifras.gob.ec/documentos/web-inec/Multiproposito/201812_Resultados_Multiproposito.pdf. [Accedido: 28-dic-2020].

[4] J. Voutssas, «Preservación documental digital y seguridad informática», vol. 24, pp. 127-155, 2010.

[5] J. Figueroa, R. Rodríguez, C. Bone, y J. Saltos, «La seguridad informática y la seguridad de la información», *Polo del Conoc.*, vol. 2, n.º 12, pp. 145-155, 2017.

[6] P. Gómez y R. Salas, «Prestación del servicio de producción de tecnología educativa con base en las buenas prácticas de la librería ITIL», *Rev. Iberoam. para la Investig. y el Desarro. Educ.*, vol. 9, n.º 18, pp. 683-716, 2019.

[7] AXELOS, «ITIL® Foundation, ITIL 4 edition», *AXELOS*, 2019. [En línea]. Disponible en: https://www.axelos.com/store/book/itil-foundation-itil-4-edition. [Accedido: 05-ene-2020].

[8] GB-Advisors, «ITIL v4: ¿ Qué novedades nos trae la nueva versión de ITIL?», *GB-Advisors*, 2019. [En línea]. Disponible en: https://www.gb-advisors.com/es/itil-v4/. [Accedido: 05-ene-2020].

[9] ISACA, «Introducing COBIT 2019», *ISACA*, n.º November, 2018.

[10] N. I. Consultores, «EL ESTÁNDAR INTERNACIONAL ISO/IEC 15504», 2018. [En línea]. Disponible en: https://www.normas-iso.com/iso-iec-15504-spice/. [Accedido: 06-ene-2021].

[11] N. I. Consultores, «ISO 20000 GESTIONANDO LA CALIDAD DE SUS SERVICIOS TI», 2018. [En línea]. Disponible en: https://www.normas-iso.com/iso-20000/. [Accedido: 06-ene-2021].

[12] C. Advisera, «Guía simplificada sobre requerimientos de ISO 20000», 2018. [En línea]. Disponible en: https://advisera.com/20000academy/es/que-es-iso-20000/. [Accedido:

07-ene-2021].

[13] I. T. Excellence, «Sistemas de Gestión de Riesgos y Seguridad ISO 27001», 2018. [En línea]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/. [Accedido: 08-ene-2021].

[14] I. T. Excellence, «La familia de normas ISO 27000», 2015. [En línea]. Disponible en: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/. [Accedido: 08-ene-2021].

[15] ISO, «ISO/IEC 27001:2013», 2018. [En línea]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. [Accedido: 08-ene-2021].

[16] Magazcitum, «ISO-27001:2013 ¿Qué hay de nuevo?», 2013. [En línea]. Disponible en: https://www.magazcitum.com.mx/?p=2397#.YAeDAOhKiUn. [Accedido: 11-ene-2021].

[17] I. T. Excellence, «¿Cuál es la estructura de la nueva norma ISO 27001 2013?», *2017*. [En línea]. Disponible en: https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/. [Accedido: 12-ene-2021].

[18] I. T. Excellence, «Anexo A en ISO 27001, objetivos de control y controles de referencia», 2020. [En línea]. Disponible en: https://www.pmg-

ssi.com/2020/03/anexo-a-en-iso-27001-objetivos-de-control-y-controles-de-referencia/#:~:text=Definición de Anexo A en,la información de nuestra organización. [Accedido: 12-ene-2021].

[19] F. Solarte, E. Edgar, y M. Benavides, «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO / IEC 27001», *Rev. Tecnológica ESPOL*, vol. 28, n.º Diciembre, pp. 492-507, 2015.

[20] ITU, «Global Cybersecurity Index (GCI) 2018», 2018.

[21] MinTel, «40 millones de ataques al Ecuador», 2019. [En línea]. Disponible en: https://www.telecomunicaciones.gob.ec/mas-de-40-millones-de-ataques-al-ecuador-neutralizados-desde-el-retiro-del-asilo-a-julian-assange/. [Accedido: 27-ene-2021].

[22] R. Kovác, «Informe de amenazas - Tercer trimestre 2020», 2020.

[23] Kaspersky, «Mapa ciberamenazas en tiempo real», 2021. [En línea]. Disponible en: https://cybermap.kaspersky.com/es/stats#country=35&type=IDS&period=w. [Accedido: 28-ene-2021].

[24] M. Paulk, B. Curtis, M. Chrissis, y C. Weber, «Capability Maturity Model for Software», *ResearchGate*, pp. 1-26, jun. 2000.

[25] Consejo Superior de Administración Electrónica del Gobierno de España., «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Método», vol. 3, 2012.

[26] Consejo Superior de Administración Electrónica del Gobierno de España., «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Catálogo de Elementos.», vol. 3, 2012.

GLOSARIO

BD	Base de Datos
CMMI	Integración de los Modelos de Madurez de Capacidades
CobiT	Objetivos de Control para las Tecnologías de la Información y Relacionadas
DevOps	Desarrollo y Operaciones
ERP	Sistema de Planificación de Recursos Empresariales
IEC	Comisión Electrotécnica Internacional
ISO	Organización Internacional para la Estandarización
ITIL	Biblioteca de Infraestructura de Tecnologías de Información
ITU	International Telecommunication Union
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
On-Premise	Instalación Local o Llave en Mano
PDCA	Planificar, Hacer, Monitorear, Actuar
PYME	Pequeña y Mediana Empresa
SaaS	Software como un Servicio
SGSI	Sistema de Gestión de Seguridad de la Información
SI	Sistema de Información
SMS	Sistema de Gestión de Servicios
Sniffing	Espionaje de tráfico de red

SPICE	Determinación de la Capacidad de Mejora del Proceso de Software
SSE-CMM	Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas
SVS	Sistema de Valores de Servicios
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y Comunicación

ANEXOS

Cláusula	ANEXO A ISO 27001	Nivel	Madurez
A5	**Políticas de Seguridad de la Información**	0.00	**Inexistente**
A5.1	**Dirección de gestión para la seguridad de la información**	0.00	Inexistente
1.-	¿Se han desarrollado y publicado políticas sobre la Seguridad de la Información, de acuerdo a los objetivos estratégicos de la organización?	0.00	Inexistente
2.-	¿Se ha definido claramente un proceso de mejora continua respecto a las políticas de Seguridad de la información de la organización?	0.00	Inexistente
A6	**Organización de la Seguridad de la Información**	0.00	**Inexistente**
A6.1	**Organización interna**	0.00	Inexistente
1.-	¿Existe una clara definición y asignación de responsabilidades respecto a las políticas de seguridad de la Información, de forma transversal en la organización?	0.00	Inexistente
2.-	¿Existe alguna segregación organizacional que permita delimitar de mejor manera las responsabilidades y privilegios respecto a la seguridad de la información	0.00	Inexistente
3.-	¿Se ha definido un procedimiento a seguir para tomar contacto con las autoridades competentes y reportar incidentes relacionados con la seguridad de la información?	0.00	Inexistente
4.-	¿Se han realizado acercamientos con entidades relacionadas con la seguridad de la información con el fin de conocer la actualidad respecto al tema?	0.00	Inexistente

5.-	¿Se han definido lineamientos para garantizar la seguridad de la información como parte de la gestión de los proyectos manejados por la organización?	0.00	Inexistente
A6.2	**Dispositivos Móviles y Teletrabajo**	0.00	Inexistente
1.-	¿Se han establecido políticas para garantizar la seguridad de la información al momento de utilizar cualquier tipo de dispositivo móvil?	0.00	Inexistente
2.-	¿Se realiza una correcta aplicación de los criterios de seguridad definidos para los accesos en modalidad de teletrabajo o trabajo remoto?	0.00	Inexistente
A7	**Seguridad en los Recursos Humanos**	0.67	**Inexistente**
A7.1	**Antes de contratar a un empleado**	1.00	Inicial
1.-	¿Se realiza un análisis detallado de la información de los candidatos?	2.00	Repetible
	-Respecto a la formación	2.00	Repetible
	-Respecto a la experiencia	2.00	Repetible
	-Se verifican las titulaciones declaradas	2.00	Repetible
	-Se contacta a referencias	2.00	Repetible
2.-	¿Los contratos, de los colaboradores, son redactados de tal forma que se incluyan cláusulas referentes a la seguridad de la información?	0.00	Inexistente
A7.2	**Durante el contrato**	0.00	Inexistente
1.-	¿Existe una exigencia activa para asegurar el cumplimiento de las políticas de seguridad de la información tanto por colaboradores como por proveedores?	0.00	Inexistente

2.-	¿Se han definido procesos de socialización, formación y sensibilización respecto a las responsabilidades que atañen a la seguridad de la información en la organización?	0.00	Inexistente
3.-	¿Se han definido sanciones, para colaboradores y proveedores, sobre las consecuencias que acarrea el incumplimiento de las políticas de seguridad de la información?	0.00	Inexistente
A7.3	**Terminación del contrato**	1.00	Inicial
1.-	¿Se ha definido un procedimiento que procure garantizar la seguridad de la información en los escenarios de cambios de cargo o puesto de trabajo o al finiquitar un contrato?	2.00	Repetible
2.-	¿Se han definido responsabilidades, respecto a la seguridad de la información, que no se extingan con la finalización de un contrato? Por ejemplo, clausulas relacionadas con la confidencialidad de la Información	0.00	Inexistente
A8	**Gestión de Activos**	0.50	**Inexistente**
A8.1	**Responsabilidad sobre los Activos**	1.50	Inicial
1.-	¿Se ha realizado el levantamiento de inventarios de activos que soportan el negocio y la información que se genera a partir de las actividades de la organización?	3.00	Definido
2.-	¿Cada uno de los activos ha sido asignado a un responsable, quien debe garantizar su seguridad e integridad?	3.00	Definido
3.-	¿Se han establecido políticas que garanticen el uso responsable de los activos de información respecto a su seguridad e integridad?	0.00	Inexistente
4.-	¿Se ha definido un procedimiento para receptar los activos que habían sido asignados a terceras personas o al momento de la extinción de una plaza de trabajo o un contrato?	0.00	Inexistente

A8.2	**Clasificación de la Información**	0.00	Inexistente
1.-	¿Existe una política de clasificación de la información, de acuerdo a su nivel de confidencialidad o importancia, con el fin de aplicar medidas de seguridad adecuadas?	0.00	Inexistente
2.-	¿Existe una manera sencilla de identificar los activos de información respecto a su nivel de confidencialidad o de clasificación?	0.00	Inexistente
3.-	¿Se han definido políticas respecto a la manipulación y tratamiento de la información, de acuerdo a las clasificaciones asignadas?	0.00	Inexistente
A8.3	**Manipulación de Soportes**	0.00	Inexistente
1.-	¿Se han desarrollado controles aplicables al uso de soportes extraíbles?	0.00	Inexistente
	-Respecto al uso	0.00	Inexistente
	-Respecto al cifrado	0.00	Inexistente
	-Respecto al borrado	0.00	Inexistente
	-Etc.	0.00	Inexistente
2.-	¿Se han establecido procedimientos para garantizar una eliminación segura de soportes extraíbles?	0.00	Inexistente
3.-	¿Se han definido procedimientos que garanticen la seguridad de los soportes extraíbles, al momento de su transporte?	0.00	Inexistente
	-Respecto al control de salidas	0.00	Inexistente
	-Respecto al Cifrado	0.00	Inexistente
	-Otros	0.00	Inexistente
A9	**Control de Acceso**	0.45	**Inexistente**
A9.1	**Requisitos generales para el control de acceso**	0.00	Inexistente

1.-	¿Se han definido políticas para la asignación de privilegios de acceso selectivo a la información, en relación a las necesidades propias de cada cargo?	0.00	Inexistente
2.-	¿Los accesos a los servicios y recursos de las redes se asignan de manera limitada y de acuerdo a las necesidades de cada cargo?	0.00	Inexistente
A9.2	**Accesos de Usuario**	1.00	Inicial
1.-	¿Se ha definido un procedimiento formal para el registro de usuarios de la organización?	2.00	Repetible
2.-	¿Se ha definido un proceso formal para realizar la asignación de los perfiles de acceso?	2.00	Repetible
3.-	¿Se ha definido un proceso específico e independiente para ejecutar la autorización y asignación de accesos especiales?	2.00	Repetible
4.-	¿Se ha definido una política clara y específica sobre la manipulación de información categorizada como secreta?	0.00	Inexistente
	-Respecto a la autenticación	0.00	Inexistente
	-Respecto a los compromisos	0.00	Inexistente
5.-	¿Se ha establecido una política de periodos de caducidad y renovación referente a los privilegios de acceso?	0.00	Inexistente
6.-	¿Se ha definido una política para la revocación de accesos y privilegios, cuando se da por finalizada una actividad puntual, una plaza de trabajo o un contrato con terceros?	0.00	Inexistente
A9.3	**Responsabilidades de los usuarios**	0.00	Inexistente
1.-	¿Se ha definido una política respecto a la creación y conservación de contraseñas de acceso?	0.00	Inexistente
A9.4	**Control de acceso a sistemas y aplicaciones**	0.80	Inexistente

1.-	¿Se han definido perfiles y niveles específicos de acceso, respecto a los sistemas y plataformas de Información, de manera restringida y de acuerdo a los perfiles de cargo?	2.00	Repetible
2.-	¿Se han definido políticas de acceso seguro, tomando en consideración máximo de intentos permitidos, controlando la información mostrada en pantalla, etc.?	0.00	Inexistente
3.-	¿Se ha definido una política de creación de contraseñas consideradas seguras?	2.00	Repetible
4.-	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad?	0.00	Inexistente
5.-	¿Se ha definido una política de restricción al acceso hacia los códigos fuente de aplicativos y, además, se lleva un control de los cambios que se realizan sobre éstos?	0.00	Inexistente
A10	**Criptografía**	0.00	**Inexistente**
A10.1	**Control criptográfico**	0.00	Inexistente
1.-	¿Se ha definido una política respecto al establecimiento y aplicación de controles criptográficos?	0.00	Inexistente
2.-	¿Se ha definido un procedimiento para el control del ciclo de vida de las claves criptográficas?	0.00	Inexistente
A11	**Seguridad Física y del entorno**	0.67	**Inexistente**
A11.1	**Áreas de Seguridad**	0.00	Inexistente
1.-	¿Se han establecido perímetros de seguridad física a los que se le apliquen condiciones especiales para el acceso?	0.00	Inexistente

2.-	¿Se ha definido un procedimiento de control de acceso por parte de personal autorizado hacia las áreas categorizadas como restringidas?	0.00	Inexistente
3.-	¿Se han definido medidas de seguridad, en las oficinas, para evitar presentar información sensible en pantallas en áreas accesibles a personas externas a la organización?	0.00	Inexistente
4.-	¿Se ha definido un procedimiento de control o supervisión sobre las actividades que el personal ejecuta en áreas categorizadas como seguras?	0.00	Inexistente
5.-	¿Se ha definido un procedimiento de controlan aplicable a las áreas de carga y descarga, en relación a la entrega y recepción de mercancías?	0.00	Inexistente
A11.2	**Seguridad de los equipos**	1.33	Inicial
1.-	¿Se toman acciones para procurar la protección los equipos de la organización, tanto de los efectos del medioambiente como de posibles accesos no autorizados?	2.00	Repetible
2.-	¿Existen mecanismos de protección, para los equipos de la organización, contra posibles fallos en el suministro eléctrico?	2.00	Repetible
3.-	¿Se han tomado medidas de protección para asegurar la integridad del cableado de suministro eléctrico y el de datos?	2.00	Repetible
4.-	¿Existe una clara planificación establecida para realizar tareas de mantenimiento preventivo y predictivo sobre los equipos de la organización?	2.00	Repetible
5.-	¿Se ha definido un procedimiento de monitoreo y control sobre la salida de equipos, aplicaciones y otros dispositivos, que pudieran contener información?	0.00	Inexistente

6.-	¿Se han definido políticas de seguridad y protección específicamente para los equipos que son utilizados fuera de las instalaciones de la organización?	0.00	Inexistente
7.-	¿Se han establecido procedimientos para la protección o eliminación de información en equipos que serán dados de baja o serán reutilizados?	0.00	Inexistente
8.-	¿Se han definido políticas que aseguren la protección de la información en los equipos, al momento que los usuarios pudieran ausentarse de su puesto de trabajo?	2.00	Repetible
9.-	¿Se han definido políticas que permitan a los colaboradores ausentarse momentánea o temporalmente, de forma segura, de sus puestos de trabajo?	2.00	Repetible
A12	**Seguridad en las Operaciones**	1.19	**Inicial**
A12.1	**Procedimientos y responsabilidades**	0.80	Inexistente
1.-	¿Los procedimientos han sido documentados formalmente y se han establecido responsabilidades sobre los mismos?	0.00	Inexistente
2.-	¿Se ha definido una política que asegure que la documentación respecto a los procedimientos se mantenga permanente actualizada?	0.00	Inexistente
3.-	¿Se ha definido un procedimiento para evaluar el posible impacto que representarían los cambios a los procedimientos, respecto a la seguridad de la información?	0.00	Inexistente
4.-	¿Se ha definido un procedimiento de control respecto el uso de los recursos tecnológicos en cuanto a la capacidad y al rendimiento los sistemas y plataformas?	2.00	Repetible

5.-	¿Existe una clara y conveniente separación entre los entornos de desarrollo, pruebas y producción?	2.00	Repetible
A12.2	**Protección contra software malicioso**	2.00	Repetible
1.-	¿Se han instalado sistemas de detección para malware o software malicioso, en los equipos de la organización?	2.00	Repetible
A12.3	**Copias de Seguridad**	0.00	Inexistente
1.-	¿La organización cuenta con un sistema para efectuar copias de seguridad, de acuerdo con las necesidades de la organización?	0.00	Inexistente
A12.4	**Registros y supervisión**	1.50	Inicial
1.-	¿Se efectúa un registro detallado de eventos? Como:	2.00	Repetible
	-Intentos de acceso exitosos y fallidos	2.00	Repetible
	-Desconexiones de plataformas y de los sistemas	2.00	Repetible
	-Log de eventos de fallo	2.00	Repetible
2.-	¿Los elementos del sistema de registros y la información generada por éste se encuentran debidamente protegidos contra accesos no autorizados?	2.00	Repetible
3.-	¿Se ejecutan rutinas de control sobre las actividades desarrollados por los administradores y operadores de los sistemas y plataformas?	2.00	Repetible
4.-	¿Se han definido procedimientos para precautelar la sincronización temporal de los elementos de los distintos sistemas?	0.00	Inexistente
A12.5	**Control del Software**	2.00	Repetible
1.-	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?	2.00	Repetible

A12.6	**Vulnerabilidad Técnica**	2.00	Repetible
1.-	¿Se han establecido mecanismos de control y protección contra vulnerabilidades técnicas (hacking ético, etc.)?	2.00	Repetible
2.-	¿Se ha establecido una política de restricción con la finalidad de que las instalaciones de software se lleven a cabo exclusivamente por personal autorizado?	2.00	Repetible
A12.7	**Auditorias de Sistemas de Información**	0.00	Inexistente
1.-	¿Se han definido los correspondientes mecanismos de auditoría respecto a las seguridades de los sistemas y plataformas?	0.00	Inexistente
2.-	¿Se han establecido protocolos dedicados para la ejecución de las auditorías, procurando reducir el impacto sobre la operación?	0.00	Inexistente
A13	**Seguridad en las Comunicaciones**	1.00	**Inicial**
A13.1	**Seguridad de Redes**	2.00	Repetible
1.-	¿Se aplican los controles pertinentes sobre el entorno de la red local, asegurando la protección de los sistemas y aplicativos expuestos en ésta?	2.00	Repetible
2.-	¿Se han establecido las condiciones de seguridad pertinentes sobre todos los servicios expuestos en la red local?	2.00	Repetible
3.-	¿Se han establecido las correspondientes separaciones o segregaciones de la red, procurando garantizar la seguridad de los activos y servicios?	2.00	Repetible
A13.2	**Intercambio de Información**	0.00	Inexistente
1.-	¿Se ha definido una política aplicable para los intercambios de información, que asegure la protección de la información compartida?	0.00	Inexistente

2.-	¿Se han establecido acuerdos de intercambio seguro aplicables a la información que se comparte con entidades externas?	0.00	Inexistente
3.-	¿Se han establecido políticas o criterios de seguridad aplicables al uso de mensajería electrónica en la organización?	0.00	Inexistente
4.-	¿Se han establecido acuerdos de confidencialidad entre la organización y las entidades externas con las que se compartirá información?	0.00	Inexistente
A14	**Adquisición, desarrollo y mantenimiento de sistemas de información**	1.85	**Inicial**
A14.1	**Intercambio de Información**	2.00	Repetible
1.-	¿Se han definido políticas respecto a los lineamientos de seguridad con la que debe cumplir cualquier nuevo sistema o aplicación?	2.00	Repetible
2.-	¿Se han definido políticas de seguridad específicas para la asignación de accesos externos o a través de redes públicas hacia los sistemas o aplicaciones internas?	2.00	Repetible
3.-	¿Se han establecido medidas de protección que garanticen la seguridad de las transacciones en línea?	2.00	Repetible
A14.2	**Seguridad en los procesos de Soporte**	1.56	Inicial
1.-	¿Se han establecido procedimientos adecuados para garantizar el desarrollo seguro de los sistemas y aplicaciones?	2.00	Repetible
2.-	¿Se han definido políticas para la gestión y control de cambios solicitados, respecto al impacto que pudieran representar para los sistemas y aplicaciones?	2.00	Repetible

3.-	¿Se han establecido procedimientos adecuados para la ejecución de verificaciones posteriores a la liberación de cambios o actualizaciones en producción?	2.00	Repetible
4.-	¿Se han establecido procedimientos formales para la gestión de actualizaciones o nuevas funcionalidades sobre sistemas provistos por terceros?	2.00	Repetible
5.-	¿Se han definido políticas, que garanticen la seguridad de la información, respecto a los procesos de ingeniería de sistemas dentro de la organización?	2.00	Repetible
6.-	¿Se ha definido un proceso evaluación de riesgos respecto a las herramientas y entornos de desarrollo de software de la organización?	0.00	Inexistente
7.-	¿Se han definido procedimientos que garanticen la seguridad de la información en los procesos de desarrollo de software llevado a cabo por terceros?	0.00	Inexistente
8.-	¿Se han definido políticas respecto a la ejecución de pruebas funcionales y de seguridad de los sistemas y aplicaciones, antes de ser liberados en producción?	2.00	Repetible
9.-	¿Se han establecido políticas respecto a los protocolos, estándares y criterios de aceptación respecto a la implementación de actualizaciones o nuevos sistemas?	2.00	Repetible
A14.3	**Datos de prueba**	2.00	Repetible
1.-	¿Se han definido políticas respecto a la designación y uso adecuado de los datos de prueba durante el desarrollo y las pruebas de los sistemas?	2.00	Repetible
A15	**Relación con Proveedores**	1.33	**Inicial**

A15.1	**Seguridad en la Relación con Proveedores**	0.67	Inexistente
1.-	¿Se han definido políticas que garanticen la seguridad de la información respecto a los accesos, hacia los activos de información, concedidos a terceros?	2.00	Repetible
2.-	¿Se han definido políticas de seguridad de la información aplicables a los contratos suscritos con terceros?	0.00	Inexistente
3.-	¿Se han definido políticas que busquen extender la seguridad de la información en relación a todas las operaciones y/o transacciones efectuadas con terceros?	0.00	Inexistente
A15.2	**Gestión de servicios externos**	2.00	Repetible
1.-	¿Se han definido procedimientos de control que garanticen el cumplimiento de las políticas establecidas para la interacción con proveedores externos?	2.00	Repetible
2.-	¿Se han definido políticas que aseguren el correspondiente análisis de impacto y gestión relacionados con los cambios sobre servicios prestados por proveedores externos?	2.00	Repetible
A16	**Gestión de incidentes de seguridad de la información**	0.57	**Inexistente**
A16.1	**Gestión de incidentes de seguridad de la información y mejoras.**	0.57	Inexistente
1.-	¿Se han documentado formalmente los procedimientos y responsabilidades en relación a la respuesta ante incidentes y eventos de la seguridad de la información?	0.00	Inexistente
2.-	¿Se han establecido los canales regulares a utilizar para la adecuada comunicación respecto incidentes y eventos que afecten la seguridad de la información?	2.00	Repetible

3.-	¿Se ha definido una política que promueva la identificación y comunicación respecto a posibles puntos vulnerables de la seguridad de la información en la organización?	0.00	Inexistente
4.-	¿Se ha definido un procedimiento para el análisis y categorización de los posibles incidentes y eventos de la seguridad de la información?	0.00	Inexistente
5.-	¿Se han definido protocolos de acción respecto a la respuesta adecuada para cada categoría de incidentes y eventos de la seguridad de la información?	2.00	Repetible
6.-	¿Se han definido procedimiento que aseguren la implementación de medidas preventivas a partir de la información provista por los eventos de la seguridad de la información?	0.00	Inexistente
7.-	¿Se ha definido un proceso unificado para la recopilación de evidencias e información relacionada con los incidentes y eventos en la seguridad de la información?	0.00	Inexistente
A17	**Gestión de la Continuidad del Negocio**	0.00	**Inexistente**
A17.1	**Continuidad de la seguridad de la información.**	0.00	Inexistente
1.-	¿Se ha definido un plan de acción que garantice la continuidad del negocio frente a posibles incidentes y eventos de seguridad de la información?	0.00	Inexistente
2.-	¿Se han implementado las medidas de recuperación, ante incidentes y eventos de seguridad de la información, descritas en el plan de continuidad del negocio?	0.00	Inexistente
3.-	¿Se han ejecutado verificaciones o pruebas sobre los procedimientos detallados en el plan de continuidad del negocio?	0.00	Inexistente
A17.2	**Redundancias**	0.00	Inexistente

1.-	¿Se ha ejecutado una evaluación detallada respecto a la necesidad de contar con redundancias para los activos de información catalogados como críticos?	0.00	Inexistente
A18	**Cumplimiento Legal y Contractual**	0.40	**Inexistente**
A18.1	**Cumplimiento de los requisitos legales y contractuales.**	0.80	Inexistente
1.-	¿Se ha ejecutado un análisis respecto a las leyes y normativas aplicables a la protección de datos personales y su cumplimiento, en el ámbito del desarrollo del negocio?	2.00	Repetible
	-Leyes aplicables al comercio electrónico	2.00	Repetible
	-Leyes aplicables a la ejecución de transacciones bancarias	2.00	Repetible
	-Leyes sobre información protegida	2.00	Repetible
	-Otras leyes propias del rubro de negocio o actividad	2.00	Repetible
	-Leyes general aplicables a las telecomunicaciones	2.00	Repetible
2.-	¿Se han implementado procedimientos que garanticen la no violentación de los derechos de propiedad intelectual de terceros?	2.00	Repetible
3.-	¿Se han establecido políticas que permitan una adecuada clasificación de la data y la aplicación de medidas las de protección pertinentes, evitando perdida, destrucción, etc.?	0.00	Inexistente
4.-	¿Se han definido medidas que garanticen la protección de datos personales, manejados por la organización, de acuerdo con las leyes y normativas aplicables?	0.00	Inexistente
5.-	¿Si han definido políticas y procedimientos de control respecto a la aplicación de cifrado criptográfico, según las leyes y reglamentos aplicables?	0.00	Inexistente
A18.2	**Revisiones de la Seguridad de la Información**	0.00	Inexistente

1.-	¿Se han definido procedimientos para la ejecución de revisiones independientes / externas sobre los controles de la seguridad de la información?	0.00	Inexistente
2.-	¿Se ejecutan revisiones periódicas respecto al adecuado cumplimiento de las políticas, procedimientos y controles sobre la seguridad de la información?	0.00	Inexistente
3.-	¿Se ejecutan evaluaciones periódicas sobre el adecuado funcionamiento de las medidas técnicas definidas para asegurar la protección de la seguridad de la información?	0.00	Inexistente

ANEXO B- INVENTARIOS DE ACTIVOS DE INFORMACIÓN					
Proceso:	Administración de Servicios SaaS				
Líder del proceso:	Jefatura de Operaciones				
Responsable:	Jefatura de Operaciones				
Elaboración:	29/6/2021				
N°	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipología**	**Custodio del activo de información**	**Localización del activo de información**
1	Red local	Puntos de red para usuarios y para para servidores.	Comunicaciones	Jefatura de Operaciones	Matriz
2	Equipo de comunicación interna o de acceso	Equipos routers y switchs cableados distribuidos en la oficina.	Comunicaciones	Jefatura de Operaciones	Matriz
3	Red inalámbrica	Equipos routers inalámbricos, distribuidos en la oficina.	Comunicaciones	Jefatura de Operaciones	Matriz
4	Equipos de comunicación core	Equipos routers cableados provistos por el proveedor ISP.	Comunicaciones	Jefatura de Operaciones	Matriz
5	Red telefónica	Comunicaciones telefónicas instaladas en la oficina.	Comunicaciones	Jefatura de Operaciones	Matriz
6	Internet	Servicio de acceso a internet, provisto por el ISP.	Comunicaciones	Jefatura de Operaciones	Matriz
7	Equipo firewall	Equipo destinado a la administración de accesos, tanto en la red local como hacia el internet.	Hardware	Jefatura de Operaciones	Matriz
8	Equipos UPS	Equipos destinados a dar respaldo energético a los servidores.	Hardware	Jefatura de Operaciones	Matriz

ANEXO B- INVENTARIOS DE ACTIVOS DE INFORMACIÓN					
Proceso:	Administración de Servicios SaaS				
Líder del proceso:	Jefatura de Operaciones				
Responsable:	Jefatura de Operaciones				
Elaboración:	29/6/2021				
N°	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipología**	**Custodio del activo de información**	**Localización del activo de información**
9	Impresoras	Equipos destinados a la impresión de documentos de uso interno.	Hardware	Equipo Servicios SaaS	Matriz
10	Laptops	Equipos asignados a los responsables de la administración SaaS.	Hardware	Equipo Servicios SaaS	Matriz
11	PCs de escritorio	Equipos asignados a los responsables de la administración SaaS.	Hardware	Equipo Servicios SaaS	Matriz
12	Servidor de aplicaciones	Equipo físico que alberga los servidores virtuales.	Hardware	Equipo Servicios SaaS	Matriz
13	Servidor de base de datos	Equipo físico que alberga los servidores virtuales.	Hardware	Equipo Servicios SaaS	Matriz
14	Servidor web	Equipo físico donde corre un servidor web.	Hardware	Equipo Servicios SaaS	Matriz

ANEXO B- INVENTARIOS DE ACTIVOS DE INFORMACIÓN					
Proceso:	Administración de Servicios SaaS				
Líder del proceso:	Jefatura de Operaciones				
Responsable:	Jefatura de Operaciones				
Elaboración:	29/6/2021				
N°	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipología**	**Custodio del activo de información**	**Localización del activo de información**
15	Credenciales de administración	Credenciales de accesos a las plataformas SaaS.	Información	Equipo Servicios SaaS	Matriz
16	Contratos SLAs	Contratos de niveles de servicio, base para la atención de novedades.	Información	Jefatura de Operaciones	Matriz
17	Esquema de base de datos Negysert	Motor de base de datos donde se almacena la data propia de Negysert.	Información	Equipo Servicios SaaS	Matriz
18	Esquemas de base de datos por cliente	Motor de base de datos donde se almacena la data de cada uno de los clientes.	Información	Equipo Servicios SaaS	Matriz
19	Ficheros de configuraciones	Fecheros donde se almacenas las configuraciones propias de cada cliente.	Información	Equipo Servicios SaaS	Matriz
20	Sistema Antivirus	Sistema encargado de detectar y eliminar virus en los PCs de usuarios.	Software	Equipo Servicios SaaS	Matriz

ANEXO B- INVENTARIOS DE ACTIVOS DE INFORMACIÓN					
Proceso:	Administración de Servicios SaaS				
Líder del proceso:	Jefatura de Operaciones				
Responsable:	Jefatura de Operaciones				
Elaboración:	29/6/2021				
N°	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipología**	**Custodio del activo de información**	**Localización del activo de información**
21	Integración sistema facturador combustibles	Integración entre el sistema despachador y facturador de combustible con Titanium SaaS.	Software	Equipo Servicios SaaS	Matriz
22	Internet corporativo	Servicio de internet provisto por ISP.	Servicios	Jefatura de Operaciones	Matriz
23	Licencias servidores Linux	Licencias de sistema operativo de los servidores de aplicaciones y de bases de datos.	Información	Jefatura de Operaciones	Matriz
24	Licencias Windows	Licencias de sistema operativo de los equipos personales.	Información	Jefatura de Operaciones	Matriz
25	Manual de usuarios ERP Titanium SaaS	Manuales de cada uno de los módulos disponibles en Titanium SaaS.	Información	Equipo Servicios SaaS	Matriz
26	Hipervisor de máquinas virtuales	Hipervisores de máquinas virtuales que alojan los servidores: vSphere Client 6.0.	Software	Equipo Servicios SaaS	Matriz
27	Ofimática	Aplicaciones de Microsoft Office.	Software	Equipo Servicios SaaS	Matriz

ANEXO B- INVENTARIOS DE ACTIVOS DE INFORMACIÓN					
Proceso:	Administración de Servicios SaaS				
Líder del proceso:	Jefatura de Operaciones				
Responsable:	Jefatura de Operaciones				
Elaboración:	29/6/2021				
N°	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipología**	**Custodio del activo de información**	**Localización del activo de información**
28	Servidor virtual de Aplication Server	Servidor virtual donde se ejecuta la máquina virtual que tiene Titanium SaaS.	Software	Equipo Servicios SaaS	Matriz
29	Servidor virtual de base de datos	Servidor virtual donde corre motor de base de datos ERP Titanium SaaS.	Software	Equipo Servicios SaaS	Matriz
30	Respaldos de base de datos	Respaldos de las bases de datos tanto internas de Negysert como de cada uno de los clientes.	Información	Equipo Servicios SaaS	Matriz
31	Respaldos de código fuentes	Respaldos de código fuentes del ERP Titanium SaaS.	Información	Equipo Servicios SaaS	Matriz
32	Servicio de correo electrónico	Servicio de correo electrónico utilizado para comunicaciones.	Servicios	Equipo Servicios SaaS	Matriz
33	Mobiliario	Equipos de oficina e insumos utilizados para el desarrollo de las actividades.	Otros	Equipo Servicios SaaS	Matriz

ANEXO B- INVENTARIOS DE ACTIVOS DE INFORMACIÓN					
Proceso:	Administración de Servicios SaaS				
Líder del proceso:	Jefatura de Operaciones				
Responsable:	Jefatura de Operaciones				
Elaboración:	29/6/2021				
N°	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipología**	**Custodio del activo de información**	**Localización del activo de información**
34	Usuarios externos	Usuarios pertenecientes a las organizaciones clientes.	Personal	Equipo Servicios SaaS	Matriz
35	Usuarios internos	Personal perteneciente a Negysert.	Personal	Equipo Servicios SaaS	Matriz
36	Personal de operaciones SaaS	Equipo de administración y soporte interno de Negysert.	Personal	Jefatura de Operaciones	Matriz
37	Oficinas Negysert	Oficinas de Negysert, ubicadas en el Condominio Orellana, en Guayaquil.	Instalaciones	Presidencia	Matriz
38	Sistema de climatización	Sistema encargado de mantener la climatización de los equipos informáticos.	Instalaciones	Jefatura de Operaciones	Matriz
39	Integración SRI	Integración SRI para generación documentos electrónicos	Software	Equipo Servicios SaaS	Matriz

ANEXO C - CATEGORIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN, SEGÚN SU CRITICIDAD							
N°	**Nombre del Activo de Información**	**Tipología**	**Confid.**	**Dispon.**	**Integr.**	**Valor**	**Importancia**
1	Red local	Comunicaciones	3	5	5	4	Alta
2	Equipo de comunicación interna o de acceso	Comunicaciones	3	4	4	4	Alta
3	Red inalámbrica	Comunicaciones	3	2	3	3	Media
4	Equipos de comunicación core	Comunicaciones	3	5	5	4	Alta
5	Red telefónica	Comunicaciones	2	2	3	2	Baja
6	Internet	Comunicaciones	2	4	2	3	Media
7	Equipo firewall	Hardware	4	5	5	5	Crítica
8	Equipos UPS	Hardware	0	3	0	1	Muy Baja
9	Impresoras	Hardware	0	1	0	0	No Aplica
10	Laptops	Hardware	3	4	4	4	Alta
11	PCs de escritorio	Hardware	3	4	4	4	Alta
12	Servidor de aplicaciones	Hardware	4	5	5	5	Crítica
13	Servidor de base de datos	Hardware	4	5	5	5	Crítica
14	Servidor web	Hardware	4	5	5	5	Crítica
15	Credenciales de administración	Información	5	5	5	5	Crítica
16	Contratos SLAs	Información	2	2	2	2	Baja
17	Esquema de base de datos Negysert	Información	5	3	5	4	Alta
18	Esquemas de base de datos por cliente	Información	5	5	5	5	Crítica

ANEXO C - CATEGORIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN, SEGÚN SU CRITICIDAD							
N°	**Nombre del Activo de Información**	**Tipología**	**Confid.**	**Dispon.**	**Integr.**	**Valor**	**Importancia**
19	Ficheros de configuraciones	Información	3	3	4	3	Media
20	Sistema Antivirus	Software	0	4	4	3	Media
21	Integración sistema facturador combustibles	Software	2	3	4	3	Media
22	Internet corporativo	Servicios	3	5	4	4	Alta
23	Licencias servidores Linux	Información	4	3	4	4	Alta
24	Licencias Windows	Información	4	3	4	4	Alta
25	Manual de usuarios ERP Titanium SaaS	Información	2	2	2	2	Baja
26	Hipervisor de máquinas virtuales	Software	4	5	5	5	Crítica
27	Ofimática	Software	2	2	2	2	Baja
28	Servidor virtual de Aplication Server	Software	4	5	5	5	Crítica
29	Servidor virtual de base de datos	Software	4	5	5	5	Crítica
30	Respaldos de base de datos	Información	4	3	5	4	Alta
31	Respaldos de código fuentes	Información	5	2	5	4	Alta
32	Servicio de correo electrónico	Servicios	4	3	4	4	Alta
33	Mobiliario	Otros	0	2	0	1	Muy Baja
34	Usuarios externos	Personal	0	0	0	0	No Aplica
35	Usuarios internos	Personal	0	0	0	0	No Aplica

ANEXO C - CATEGORIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN, SEGÚN SU CRITICIDAD							
N°	**Nombre del Activo de Información**	**Tipología**	**Confid.**	**Dispon.**	**Integr.**	**Valor**	**Importancia**
36	Personal de operaciones SaaS	Personal	0	5	0	2	Baja
37	Oficinas Negysert	Instalaciones	0	3	0	1	Muy Baja
38	Sistema de climatización	Instalaciones	0	4	0	1	Muy Baja
39	Integración SRI	Software	2	3	5	3	Media

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
CO	Accidental	Falla técnica	No disponibilidad de equipos o instalaciones.
HW	Accidental	Falla técnica	No disponibilidad de equipos o instalaciones.
CO	Accidental	Falla técnica	Procedimientos de mantenimiento, de instalaciones y equipos, no adecuado o inexistente.
HW	Accidental	Falla técnica	Procedimientos de mantenimiento, de instalaciones y equipos, no adecuado o inexistente.
CO	Accidental	Falla técnica	Inadecuada o inexistente política de control sobre los cambios.
HW	Accidental	Falla técnica	Inadecuada o inexistente política de control sobre los cambios.
HW	Accidental	Falla técnica	Procedimientos de monitoreo inadecuados o inexistentes, respecto al hardware.
CO	Accidental	Falla técnica	Procedimientos de monitoreo inadecuados o inexistentes, respecto al hardware.
HW	Accidental	Falla técnica	Inadecuados o inexistentes procedimientos para una adecuada estimación de la capacidad de cómputo necesaria.
CO	Accidental	Falla técnica	Inadecuados o inexistentes procedimientos para una adecuada estimación de la capacidad de cómputo necesaria.
HW	Accidental	Falla técnica	Inadecuado o inexistente plan de continuidad.
CO	Accidental	Falla técnica	Inadecuado o inexistente plan de continuidad.
HW	Accidental	Falla técnica	Inadecuado o inexistente plan de recuperación.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
CO	Accidental	Falla técnica	Inadecuado o inexistente plan de recuperación.
HW	Deliberada	Datos accedidos sin autorización	Inadecuada o inexistente política de manipulación de equipos.
CO	Deliberada	Datos accedidos sin autorización	Inadecuada o inexistente política de manipulación de equipos.
HW	Deliberada	Sabotaje	Inadecuada o inexistente política de control de accesos.
CO	Deliberada	Sabotaje	Inadecuada o inexistente política de control de accesos.
IN	Deliberada	Sabotaje	Inadecuada o inexistente política de control de accesos.
HW	Deliberada	Sabotaje	Inadecuada o inexistente seguridad física de las instalaciones.
CO	Deliberada	Sabotaje	Inadecuada o inexistente seguridad física de las instalaciones.
IN	Deliberada	Sabotaje	Inadecuada o inexistente seguridad física de las instalaciones.
HW	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente plan de continuidad.
CO	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente plan de continuidad.
IN	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente plan de continuidad.
HW	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente plan de recuperación.
CO	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente plan de recuperación.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
IN	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente plan de recuperación.
HW	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente sistema de regulación de voltaje eléctrico.
CO	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente sistema de regulación de voltaje eléctrico.
IN	Entorno	Variaciones de voltaje eléctrico	Inadecuado o inexistente sistema de regulación de voltaje eléctrico.
SW	Deliberada	Acceso no presencial sin autorización	Inadecuada o inexistente política de control de accesos remotos.
CO	Deliberada	Acceso no presencial sin autorización	Inadecuada o inexistente política de control de accesos remotos.
IF	Deliberada	Acceso no presencial sin autorización	Inadecuada o inexistente política de control de accesos remotos.
CO	Deliberada	Sniffing	Inadecuado o inexistente aseguramiento físico de los equipos de comunicaciones y su cableado.
IN	Deliberada	Sniffing	Inadecuado o inexistente aseguramiento físico de los equipos de comunicaciones y su cableado.
IF	Deliberada	Sniffing	Inadecuado o inexistente aseguramiento físico de los equipos de comunicaciones y su cableado.
CO	Deliberada	Sniffing	Inadecuada o inexistente política de cifrado en las comunicaciones.
IF	Deliberada	Sniffing	Inadecuada o inexistente política de cifrado en las comunicaciones.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
CO	Deliberada	Sniffing	Inadecuada o inexistente segmentación física y lógica en la red de comunicaciones.
IF	Deliberada	Destrucción de información	Inadecuada o inexistente política de control de accesos.
HW	Deliberada	Destrucción de información	Inadecuada o inexistente política de control de accesos.
IN	Deliberada	Destrucción de información	Inadecuada o inexistente política de control de accesos.
SR	Deliberada	Destrucción de información	Inadecuada o inexistente política de control de accesos.
IF	Entorno	Inundación	Desconocimiento de inundabilidad de la zona de las instalaciones.
CO	Entorno	Inundación	Desconocimiento de inundabilidad de la zona de las instalaciones.
HW	Entorno	Inundación	Desconocimiento de inundabilidad de la zona de las instalaciones.
IN	Entorno	Inundación	Desconocimiento de inundabilidad de la zona de las instalaciones.
SR	Entorno	Inundación	Desconocimiento de inundabilidad de la zona de las instalaciones.
IF	Deliberada	Filtración de información	Inadecuada o inexistente política disciplinaria y regulatoria.
PE	Deliberada	Filtración de información	Inadecuada o inexistente política disciplinaria y regulatoria.
IF	Deliberada	Filtración de información	Inadecuada o inexistente socialización de la política disciplinaria y regulatoria.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
PE	Deliberada	Filtración de información	Inadecuada o inexistente socialización de la política disciplinaria y regulatoria.
IF	Deliberada	Filtración de información	Inadecuada o inexistente entrenamiento en seguridad informática.
PE	Deliberada	Filtración de información	Inadecuada o inexistente entrenamiento en seguridad informática.
IF	Deliberada	Manipulación indebida de la información	Inadecuada o inexistente política disciplinaria y regulatoria.
PE	Deliberada	Manipulación indebida de la información	Inadecuada o inexistente política disciplinaria y regulatoria.
SE	Deliberada	Manipulación indebida de la información	Inadecuada o inexistente política disciplinaria y regulatoria.
PE	Accidental	Personal no idóneo	Inadecuada o inexistente política de vinculación de empleados.
PE	Deliberada	Corrupción	Inadecuada o inexistente política disciplinaria y regulatoria.
PE	Deliberada	Ausencia de colaborador clave	Inadecuada o inexistente reemplazo y transferencia de responsabilidades.
PE	Deliberada	Ingeniería social	Inadecuada o inexistente socialización de riegos informáticos.
SE	Deliberada	Ingeniería social	Inadecuada o inexistente socialización de riegos informáticos.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
SE	Accidental	Recuperación extemporánea de servicios	Inadecuados o inexistentes SLAs con los proveedores de servicios.
SE	Accidental	Deterioro de servicios provistos por terceros	Inadecuados o inexistentes SLAs con los proveedores de servicios.
SE	Accidental	Denegación de servicios	Inadecuados o inexistentes SLAs con los proveedores de servicios.
SE	Deliberada	Sabotaje	Inadecuados o inexistentes SLAs con los proveedores de servicios.
SW	Accidental	Problemas con los servicios de comunicación	Inadecuado o inexistente aseguramiento físico de los equipos de comunicaciones y su cableado.
CO	Accidental	Problemas con los servicios de comunicación	Inadecuado o inexistente aseguramiento físico de los equipos de comunicaciones y su cableado.
SW	Accidental	Problemas con los servicios de comunicación	Capacidad planificada excedida.
CO	Accidental	Problemas con los servicios de comunicación	Capacidad planificada excedida.
SW	Accidental	Problemas con los servicios de comunicación	Inadecuado o inexistente servicio alterno de comunicación.
CO	Accidental	Problemas con los servicios de comunicación	Inadecuado o inexistente servicio alterno de comunicación.
SW	Accidental	Falla técnica en SW	Inadecuado o inexistente procedimiento de actualización.
IF	Accidental	Falla técnica en SW	Inadecuado o inexistente procedimiento de actualización.
SW	Deliberada	Acceso no autorizado	Inadecuado o inexistente perfilamiento en los sistemas.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
IF	Deliberada	Acceso no autorizado	Inadecuado o inexistente perfilamiento en los sistemas.
SW	Deliberada	Manipulación indebida de la información	Inadecuado o inexistente perfilamiento en los sistemas.
IF	Deliberada	Manipulación indebida de la información	Inadecuado o inexistente perfilamiento en los sistemas.
SW	Deliberada	Manipulación indebida de la información	Inadecuado o inexistente aislamiento de ambientes de desarrollo.
IF	Deliberada	Manipulación indebida de la información	Inadecuado o inexistente aislamiento de ambientes de desarrollo.
SW	Accidental	Debilidades de SW	Inadecuado o inexistente proceso de levantamiento de requerimientos.
IF	Accidental	Debilidades de SW	Inadecuado o inexistente proceso de levantamiento de requerimientos.
SW	Accidental	Debilidades de SW	Personal no idóneo para el desarrollo de SW.
IF	Accidental	Debilidades de SW	Personal no idóneo para el desarrollo de SW.
SW	Accidental	Debilidades de SW	Inadecuada o inexistente metodología de desarrollo de SW.
IF	Accidental	Debilidades de SW	Inadecuada o inexistente metodología de desarrollo de SW.
SW	Accidental	Debilidades de SW	Inadecuada o inexistente estándares de seguridad en el desarrollo de SW.
IF	Accidental	Debilidades de SW	Inadecuada o inexistente estándares de seguridad en el desarrollo de SW.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
SW	Accidental	Debilidades de SW	Inadecuada o inexistente política de control de cambios.
IF	Accidental	Debilidades de SW	Inadecuada o inexistente política de control de cambios.
SW	Deliberada	Uso de SW no autorizado	Inadecuada o inexistente política de control y distribución de SW.
IF	Deliberada	Uso de SW no autorizado	Inadecuada o inexistente política de control y distribución de SW.
IF	Entorno	Inundación	Pérdida total o parcial de los activos de información
CO	Entorno	Inundación	Pérdida total o parcial de los activos de información
HW	Entorno	Inundación	Pérdida total o parcial de los activos de información
IN	Entorno	Inundación	Pérdida total o parcial de los activos de información
SR	Entorno	Inundación	Pérdida total o parcial de los activos de información
OT	Entorno	Inundación	Pérdida total o parcial de los activos de información
IF	Entorno	Incendio	Pérdida total o parcial de los activos de información
CO	Entorno	Incendio	Pérdida total o parcial de los activos de información
HW	Entorno	Incendio	Pérdida total o parcial de los activos de información
IN	Entorno	Incendio	Pérdida total o parcial de los activos de información
SR	Entorno	Incendio	Pérdida total o parcial de los activos de información
OT	Entorno	Incendio	Pérdida total o parcial de los activos de información
IF	Deliberada	Software malicioso	Inadecuada o inexistente política de uso de medios extraíbles.
CO	Deliberada	Software malicioso	Inadecuada o inexistente política de uso de medios extraíbles.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
HW	Deliberada	Software malicioso	Inadecuada o inexistente política de uso de medios extraíbles.
SR	Deliberada	Software malicioso	Inadecuada o inexistente política de uso de medios extraíbles.
IF	Accidental	Errores de operador y usuario	Inadecuados o inexistentes manuales de usuario.
SW	Accidental	Errores de operador y usuario	Inadecuados o inexistentes manuales de usuario.
HW	Accidental	Errores de operador y usuario	Inadecuados o inexistentes manuales de usuario.
IF	Deliberada	Fraude y robo	Inadecuada o inexistente generación de logs de auditoría.
SW	Deliberada	Fraude y robo	Inadecuada o inexistente generación de logs de auditoría.
IF	Deliberada	Fraude y robo	Inadecuada o inexistente segregación de funciones de acuerdo a perfiles de cargo.
SW	Deliberada	Fraude y robo	Inadecuada o inexistente segregación de funciones de acuerdo a perfiles de cargo.
PE	Deliberada	Fraude y robo	Inadecuada o inexistente segregación de funciones de acuerdo a perfiles de cargo.
IF	Deliberada	Intrusión web	Inadecuada o inexistente configuración de reglas de firewall.
SW	Deliberada	Intrusión web	Inadecuada o inexistente configuración de reglas de firewall.
IF	Deliberada	Ausencia de colaborador clave	Inadecuada o inexistente documentación de procesos de la organización.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
CO	Deliberada	Ausencia de colaborador clave	Inadecuada o inexistente documentación de procesos de la organización.
SW	Deliberada	Ausencia de colaborador clave	Inadecuada o inexistente documentación de procesos de la organización.
HW	Deliberada	Ausencia de colaborador clave	Inadecuada o inexistente documentación de procesos de la organización.
SR	Deliberada	Ausencia de colaborador clave	Inadecuada o inexistente documentación de procesos de la organización.
PE	Deliberada	Ausencia de colaborador clave	Inadecuada o inexistente documentación de procesos de la organización.
IF	Entorno	Incendio	Inadecuada manipulación y almacenaje de materiales inflamables.
CO	Entorno	Incendio	Inadecuada manipulación y almacenaje de materiales inflamables.
SW	Entorno	Incendio	Inadecuada manipulación y almacenaje de materiales inflamables.
HW	Entorno	Incendio	Inadecuada manipulación y almacenaje de materiales inflamables.
SR	Entorno	Incendio	Inadecuada manipulación y almacenaje de materiales inflamables.
PE	Entorno	Incendio	Inadecuada manipulación y almacenaje de materiales inflamables.

ANEXO D - IDENTIFICACIÓN DE LAS AMENAZAS			
Activo Afectado	**Tipo de Amenaza**	**Amenaza**	**Vulnerabilidad**
OT	Entorno	Incendio	Inadecuada manipulación y almacenaje de materiales inflamables.
IF	Entorno	Incendio	Inadecuado o inexistente sistema de prevención y control de incendios.
CO	Entorno	Incendio	Inadecuado o inexistente sistema de prevención y control de incendios.
SW	Entorno	Incendio	Inadecuado o inexistente sistema de prevención y control de incendios.
HW	Entorno	Incendio	Inadecuado o inexistente sistema de prevención y control de incendios.
SR	Entorno	Incendio	Inadecuado o inexistente sistema de prevención y control de incendios.
PE	Entorno	Incendio	Inadecuado o inexistente sistema de prevención y control de incendios.
HW	Entorno	Humedad / temperaturas elevadas	Inadecuada o inexistente protección contra efectos ambientales.
CO	Entorno	Humedad / temperaturas elevadas	Inadecuada o inexistente protección contra efectos ambientales.
IF	Entorno	Humedad / temperaturas elevadas	Inadecuada o inexistente protección contra efectos ambientales.

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Red local	CO	Acceso no presencial sin autorización	2	3	Medio
Riesgo operativo	Red local	CO	Ausencia de colaborador clave	2	2	Aceptable
Riesgo operativo	Red local	CO	Datos accedidos sin autorización	2	2	Aceptable
Riesgo tecnológico	Red local	CO	Falla técnica	2	3	Medio
Riesgo operativo	Red local	CO	Humedad / temperaturas elevadas	3	2	Medio
Riesgo financiero	Red local	CO	Incendio	2	4	Medio
Riesgo financiero	Red local	CO	Inundación	1	4	Aceptable
Riesgo tecnológico	Red local	CO	Problemas con los servicios de comunicación	2	2	Aceptable
Riesgo financiero	Red local	CO	Sabotaje	2	3	Medio
Riesgo tecnológico	Red local	CO	Sniffing	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Red local	CO	Software malicioso	3	2	Medio
Riesgo tecnológico	Red local	CO	Variaciones de voltaje eléctrico	2	3	Medio
Riesgo financiero	Equipo de comunicación interna o de acceso	CO	Acceso no presencial sin autorización	2	3	Medio
Riesgo operativo	Equipo de comunicación interna o de acceso	CO	Ausencia de colaborador clave	2	2	Aceptable
Riesgo operativo	Equipo de comunicación interna o de acceso	CO	Datos accedidos sin autorización	2	2	Aceptable
Riesgo tecnológico	Equipo de comunicación interna o de acceso	CO	Falla técnica	2	3	Medio
Riesgo operativo	Equipo de comunicación interna o de acceso	CO	Humedad / temperaturas elevadas	3	2	Medio
Riesgo financiero	Equipo de comunicación interna o de acceso	CO	Incendio	2	4	Medio
Riesgo financiero	Equipo de comunicación interna o de acceso	CO	Inundación	1	4	Aceptable
Riesgo tecnológico	Equipo de comunicación interna o de acceso	CO	Problemas con los servicios de comunicación	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Equipo de comunicación interna o de acceso	CO	Sabotaje	2	3	Medio
Riesgo tecnológico	Equipo de comunicación interna o de acceso	CO	Sniffing	2	2	Aceptable
Riesgo tecnológico	Equipo de comunicación interna o de acceso	CO	Software malicioso	3	2	Medio
Riesgo tecnológico	Equipo de comunicación interna o de acceso	CO	Variaciones de voltaje eléctrico	2	3	Medio
Riesgo financiero	Red inalámbrica	CO	Acceso no presencial sin autorización	2	3	Medio
Riesgo operativo	Red inalámbrica	CO	Ausencia de colaborador clave	2	2	Aceptable
Riesgo operativo	Red inalámbrica	CO	Datos accedidos sin autorización	2	2	Aceptable
Riesgo tecnológico	Red inalámbrica	CO	Falla técnica	2	3	Medio
Riesgo operativo	Red inalámbrica	CO	Humedad / temperaturas elevadas	3	2	Medio
Riesgo financiero	Red inalámbrica	CO	Incendio	2	4	Medio

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Red inalámbrica	CO	Inundación	1	4	Aceptable
Riesgo tecnológico	Red inalámbrica	CO	Problemas con los servicios de comunicación	2	2	Aceptable
Riesgo financiero	Red inalámbrica	CO	Sabotaje	2	3	Medio
Riesgo tecnológico	Red inalámbrica	CO	Sniffing	2	2	Aceptable
Riesgo tecnológico	Red inalámbrica	CO	Software malicioso	3	2	Medio
Riesgo tecnológico	Red inalámbrica	CO	Variaciones de voltaje eléctrico	2	3	Medio
Riesgo financiero	Equipos de comunicación core	CO	Acceso no presencial sin autorización	2	3	Medio
Riesgo operativo	Equipos de comunicación core	CO	Ausencia de colaborador clave	2	2	Aceptable
Riesgo operativo	Equipos de comunicación core	CO	Datos accedidos sin autorización	2	2	Aceptable
Riesgo tecnológico	Equipos de comunicación core	CO	Falla técnica	2	3	Medio

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Equipos de comunicación core	CO	Humedad / temperaturas elevadas	3	2	Medio
Riesgo financiero	Equipos de comunicación core	CO	Incendio	2	4	Medio
Riesgo financiero	Equipos de comunicación core	CO	Inundación	1	4	Aceptable
Riesgo tecnológico	Equipos de comunicación core	CO	Problemas con los servicios de comunicación	2	2	Aceptable
Riesgo financiero	Equipos de comunicación core	CO	Sabotaje	2	3	Medio
Riesgo tecnológico	Equipos de comunicación core	CO	Sniffing	2	2	Aceptable
Riesgo tecnológico	Equipos de comunicación core	CO	Software malicioso	3	2	Medio
Riesgo tecnológico	Equipos de comunicación core	CO	Variaciones de voltaje eléctrico	2	3	Medio
Riesgo financiero	Red telefónica	CO	Acceso no presencial sin autorización	1	2	Aceptable
Riesgo operativo	Red telefónica	CO	Ausencia de colaborador clave	2	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Red telefónica	CO	Datos accedidos sin autorización	2	1	Aceptable
Riesgo tecnológico	Red telefónica	CO	Falla técnica	2	2	Aceptable
Riesgo operativo	Red telefónica	CO	Humedad / temperaturas elevadas	3	1	Aceptable
Riesgo financiero	Red telefónica	CO	Incendio	2	2	Aceptable
Riesgo financiero	Red telefónica	CO	Inundación	1	2	Aceptable
Riesgo tecnológico	Red telefónica	CO	Problemas con los servicios de comunicación	2	2	Aceptable
Riesgo financiero	Red telefónica	CO	Sabotaje	1	2	Aceptable
Riesgo tecnológico	Red telefónica	CO	Sniffing	1	1	Aceptable
Riesgo tecnológico	Red telefónica	CO	Software malicioso	1	1	Aceptable
Riesgo tecnológico	Red telefónica	CO	Variaciones de voltaje eléctrico	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Internet	CO	Acceso no presencial sin autorización	2	3	Medio
Riesgo operativo	Internet	CO	Ausencia de colaborador clave	2	2	Aceptable
Riesgo operativo	Internet	CO	Datos accedidos sin autorización	2	2	Aceptable
Riesgo tecnológico	Internet	CO	Falla técnica	2	3	Medio
Riesgo operativo	Internet	CO	Humedad / temperaturas elevadas	3	2	Medio
Riesgo financiero	Internet	CO	Incendio	2	4	Medio
Riesgo financiero	Internet	CO	Inundación	1	4	Aceptable
Riesgo tecnológico	Internet	CO	Problemas con los servicios de comunicación	2	2	Aceptable
Riesgo financiero	Internet	CO	Sabotaje	2	3	Medio
Riesgo tecnológico	Internet	CO	Sniffing	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Internet	CO	Software malicioso	3	2	Medio
Riesgo tecnológico	Internet	CO	Variaciones de voltaje eléctrico	2	3	Medio
Riesgo operativo	Equipo firewall	HW	Ausencia de colaborador clave	2	3	Medio
Riesgo operativo	Equipo firewall	HW	Datos accedidos sin autorización	2	3	Medio
Riesgo financiero	Equipo firewall	HW	Destrucción de información	2	3	Medio
Riesgo operativo	Equipo firewall	HW	Errores de operador y usuario	4	1	Aceptable
Riesgo tecnológico	Equipo firewall	HW	Falla técnica	2	3	Medio
Riesgo operativo	Equipo firewall	HW	Humedad / temperaturas elevadas	3	1	Aceptable
Riesgo financiero	Equipo firewall	HW	Incendio	2	4	Medio
Riesgo financiero	Equipo firewall	HW	Inundación	1	4	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Equipo firewall	HW	Sabotaje	2	3	Medio
Riesgo tecnológico	Equipo firewall	HW	Software malicioso	3	3	Medio
Riesgo tecnológico	Equipo firewall	HW	Variaciones de voltaje eléctrico	2	2	Aceptable
Riesgo operativo	Equipos UPS	HW	Ausencia de colaborador clave	1	1	Aceptable
Riesgo operativo	Equipos UPS	HW	Datos accedidos sin autorización	1	1	Aceptable
Riesgo financiero	Equipos UPS	HW	Destrucción de información	1	1	Aceptable
Riesgo operativo	Equipos UPS	HW	Errores de operador y usuario	1	1	Aceptable
Riesgo tecnológico	Equipos UPS	HW	Falla técnica	3	2	Medio
Riesgo operativo	Equipos UPS	HW	Humedad / temperaturas elevadas	3	2	Medio
Riesgo financiero	Equipos UPS	HW	Incendio	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Equipos UPS	HW	Inundación	1	2	Aceptable
Riesgo financiero	Equipos UPS	HW	Sabotaje	1	1	Aceptable
Riesgo tecnológico	Equipos UPS	HW	Software malicioso	1	1	Aceptable
Riesgo tecnológico	Equipos UPS	HW	Variaciones de voltaje eléctrico	2	2	Aceptable
Riesgo operativo	Laptops	HW	Ausencia de colaborador clave	2	1	Aceptable
Riesgo operativo	Laptops	HW	Datos accedidos sin autorización	3	2	Medio
Riesgo financiero	Laptops	HW	Destrucción de información	2	2	Aceptable
Riesgo operativo	Laptops	HW	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	Laptops	HW	Falla técnica	2	2	Aceptable
Riesgo operativo	Laptops	HW	Humedad / temperaturas elevadas	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Laptops	HW	Incendio	1	2	Aceptable
Riesgo financiero	Laptops	HW	Inundación	1	2	Aceptable
Riesgo financiero	Laptops	HW	Sabotaje	2	2	Aceptable
Riesgo tecnológico	Laptops	HW	Software malicioso	3	2	Medio
Riesgo tecnológico	Laptops	HW	Variaciones de voltaje eléctrico	2	2	Aceptable
Riesgo operativo	PCs de escritorio	HW	Ausencia de colaborador clave	2	1	Aceptable
Riesgo operativo	PCs de escritorio	HW	Datos accedidos sin autorización	3	2	Medio
Riesgo financiero	PCs de escritorio	HW	Destrucción de información	2	2	Aceptable
Riesgo operativo	PCs de escritorio	HW	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	PCs de escritorio	HW	Falla técnica	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	PCs de escritorio	HW	Humedad / temperaturas elevadas	2	2	Aceptable
Riesgo financiero	PCs de escritorio	HW	Incendio	1	2	Aceptable
Riesgo financiero	PCs de escritorio	HW	Inundación	1	2	Aceptable
Riesgo financiero	PCs de escritorio	HW	Sabotaje	2	2	Aceptable
Riesgo tecnológico	PCs de escritorio	HW	Software malicioso	3	2	Medio
Riesgo tecnológico	PCs de escritorio	HW	Variaciones de voltaje eléctrico	2	2	Aceptable
Riesgo operativo	Servidor de aplicaciones	HW	Ausencia de colaborador clave	2	2	Aceptable
Riesgo operativo	Servidor de aplicaciones	HW	Datos accedidos sin autorización	4	3	Alto
Riesgo financiero	Servidor de aplicaciones	HW	Destrucción de información	2	4	Medio
Riesgo operativo	Servidor de aplicaciones	HW	Errores de operador y usuario	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Servidor de aplicaciones	HW	Falla técnica	2	3	Medio
Riesgo operativo	Servidor de aplicaciones	HW	Humedad / temperaturas elevadas	2	3	Medio
Riesgo financiero	Servidor de aplicaciones	HW	Incendio	1	4	Aceptable
Riesgo financiero	Servidor de aplicaciones	HW	Inundación	1	4	Aceptable
Riesgo financiero	Servidor de aplicaciones	HW	Sabotaje	2	4	Medio
Riesgo tecnológico	Servidor de aplicaciones	HW	Software malicioso	4	3	Alto
Riesgo tecnológico	Servidor de aplicaciones	HW	Variaciones de voltaje eléctrico	2	2	Aceptable
Riesgo operativo	Servidor de base de datos	HW	Ausencia de colaborador clave	2	2	Aceptable
Riesgo operativo	Servidor de base de datos	HW	Datos accedidos sin autorización	4	3	Alto
Riesgo financiero	Servidor de base de datos	HW	Destrucción de información	2	4	Medio

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Servidor de base de datos	HW	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	Servidor de base de datos	HW	Falla técnica	2	3	Medio
Riesgo operativo	Servidor de base de datos	HW	Humedad / temperaturas elevadas	2	3	Medio
Riesgo financiero	Servidor de base de datos	HW	Incendio	1	4	Aceptable
Riesgo financiero	Servidor de base de datos	HW	Inundación	1	4	Aceptable
Riesgo financiero	Servidor de base de datos	HW	Sabotaje	2	4	Medio
Riesgo tecnológico	Servidor de base de datos	HW	Software malicioso	4	3	Alto
Riesgo tecnológico	Servidor de base de datos	HW	Variaciones de voltaje eléctrico	2	2	Aceptable
Riesgo operativo	Servidor web	HW	Ausencia de colaborador clave	2	2	Aceptable
Riesgo operativo	Servidor web	HW	Datos accedidos sin autorización	4	3	Alto

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Servidor web	HW	Destrucción de información	3	3	Medio
Riesgo operativo	Servidor web	HW	Errores de operador y usuario	3	2	Medio
Riesgo tecnológico	Servidor web	HW	Falla técnica	2	3	Medio
Riesgo operativo	Servidor web	HW	Humedad / temperaturas elevadas	2	3	Medio
Riesgo financiero	Servidor web	HW	Incendio	1	4	Aceptable
Riesgo financiero	Servidor web	HW	Inundación	1	4	Aceptable
Riesgo financiero	Servidor web	HW	Sabotaje	2	4	Medio
Riesgo tecnológico	Servidor web	HW	Software malicioso	4	3	Alto
Riesgo tecnológico	Servidor web	HW	Variaciones de voltaje eléctrico	2	2	Aceptable
Riesgo financiero	Credenciales de administración	IF	Acceso no autorizado	1	3	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Credenciales de administración	IF	Acceso no presencial sin autorización	3	3	Medio
Riesgo operativo	Credenciales de administración	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Credenciales de administración	IF	Debilidades de SW	3	3	Medio
Riesgo financiero	Credenciales de administración	IF	Destrucción de información	2	2	Aceptable
Riesgo operativo	Credenciales de administración	IF	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	Credenciales de administración	IF	Falla técnica en SW	3	2	Medio
Riesgo financiero	Credenciales de administración	IF	Filtración de información	2	2	Aceptable
Riesgo financiero	Credenciales de administración	IF	Fraude y robo	2	3	Medio
Riesgo operativo	Credenciales de administración	IF	Humedad / temperaturas elevadas	2	1	Aceptable
Riesgo financiero	Credenciales de administración	IF	Incendio	1	4	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Credenciales de administración	IF	Intrusión web	3	2	Medio
Riesgo financiero	Credenciales de administración	IF	Inundación	1	4	Aceptable
Riesgo financiero	Credenciales de administración	IF	Manipulación indebida de la información	3	2	Medio
Riesgo tecnológico	Credenciales de administración	IF	Sniffing	3	3	Medio
Riesgo tecnológico	Credenciales de administración	IF	Software malicioso	3	1	Aceptable
Riesgo tecnológico	Credenciales de administración	IF	Uso de SW no autorizado	3	1	Aceptable
Riesgo financiero	Contratos SLAs	IF	Acceso no autorizado	1	1	Aceptable
Riesgo financiero	Contratos SLAs	IF	Acceso no presencial sin autorización	3	1	Aceptable
Riesgo operativo	Contratos SLAs	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Contratos SLAs	IF	Debilidades de SW	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Contratos SLAs	IF	Destrucción de información	2	2	Aceptable
Riesgo operativo	Contratos SLAs	IF	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	Contratos SLAs	IF	Falla técnica en SW	3	1	Aceptable
Riesgo financiero	Contratos SLAs	IF	Filtración de información	2	2	Aceptable
Riesgo financiero	Contratos SLAs	IF	Fraude y robo	2	1	Aceptable
Riesgo operativo	Contratos SLAs	IF	Humedad / temperaturas elevadas	2	1	Aceptable
Riesgo financiero	Contratos SLAs	IF	Incendio	1	4	Aceptable
Riesgo tecnológico	Contratos SLAs	IF	Intrusión web	3	1	Aceptable
Riesgo financiero	Contratos SLAs	IF	Inundación	1	4	Aceptable
Riesgo financiero	Contratos SLAs	IF	Manipulación indebida de la información	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Contratos SLAs	IF	Sniffing	3	1	Aceptable
Riesgo tecnológico	Contratos SLAs	IF	Software malicioso	3	1	Aceptable
Riesgo tecnológico	Contratos SLAs	IF	Uso de SW no autorizado	3	1	Aceptable
Riesgo financiero	Esquema de base de datos Negysert	IF	Acceso no autorizado	2	3	Medio
Riesgo financiero	Esquema de base de datos Negysert	IF	Acceso no presencial sin autorización	3	2	Medio
Riesgo operativo	Esquema de base de datos Negysert	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Esquema de base de datos Negysert	IF	Debilidades de SW	2	3	Medio
Riesgo financiero	Esquema de base de datos Negysert	IF	Destrucción de información	2	3	Medio
Riesgo operativo	Esquema de base de datos Negysert	IF	Errores de operador y usuario	2	2	Aceptable
Riesgo tecnológico	Esquema de base de datos Negysert	IF	Falla técnica en SW	3	2	Medio

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Esquema de base de datos Negysert	IF	Filtración de información	2	2	Aceptable
Riesgo financiero	Esquema de base de datos Negysert	IF	Fraude y robo	2	2	Aceptable
Riesgo operativo	Esquema de base de datos Negysert	IF	Humedad / temperaturas elevadas	2	1	Aceptable
Riesgo financiero	Esquema de base de datos Negysert	IF	Incendio	1	4	Aceptable
Riesgo tecnológico	Esquema de base de datos Negysert	IF	Intrusión web	3	3	Medio
Riesgo financiero	Esquema de base de datos Negysert	IF	Inundación	1	4	Aceptable
Riesgo financiero	Esquema de base de datos Negysert	IF	Manipulación indebida de la información	3	2	Medio
Riesgo tecnológico	Esquema de base de datos Negysert	IF	Sniffing	3	2	Medio
Riesgo tecnológico	Esquema de base de datos Negysert	IF	Software malicioso	4	3	Alto
Riesgo tecnológico	Esquema de base de datos Negysert	IF	Uso de SW no autorizado	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Esquemas de base de datos por cliente	IF	Acceso no autorizado	2	3	Medio
Riesgo financiero	Esquemas de base de datos por cliente	IF	Acceso no presencial sin autorización	3	3	Medio
Riesgo operativo	Esquemas de base de datos por cliente	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Esquemas de base de datos por cliente	IF	Debilidades de SW	2	3	Medio
Riesgo financiero	Esquemas de base de datos por cliente	IF	Destrucción de información	2	3	Medio
Riesgo operativo	Esquemas de base de datos por cliente	IF	Errores de operador y usuario	3	3	Medio
Riesgo tecnológico	Esquemas de base de datos por cliente	IF	Falla técnica en SW	3	3	Medio
Riesgo financiero	Esquemas de base de datos por cliente	IF	Filtración de información	2	3	Medio
Riesgo financiero	Esquemas de base de datos por cliente	IF	Fraude y robo	2	3	Medio
Riesgo operativo	Esquemas de base de datos por cliente	IF	Humedad / temperaturas elevadas	2	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Esquemas de base de datos por cliente	IF	Incendio	1	4	Aceptable
Riesgo tecnológico	Esquemas de base de datos por cliente	IF	Intrusión web	3	3	Medio
Riesgo financiero	Esquemas de base de datos por cliente	IF	Inundación	1	4	Aceptable
Riesgo financiero	Esquemas de base de datos por cliente	IF	Manipulación indebida de la información	3	3	Medio
Riesgo tecnológico	Esquemas de base de datos por cliente	IF	Sniffing	3	3	Medio
Riesgo tecnológico	Esquemas de base de datos por cliente	IF	Software malicioso	4	3	Alto
Riesgo tecnológico	Esquemas de base de datos por cliente	IF	Uso de SW no autorizado	3	2	Medio
Riesgo financiero	Ficheros de configuraciones	IF	Acceso no autorizado	1	3	Aceptable
Riesgo financiero	Ficheros de configuraciones	IF	Acceso no presencial sin autorización	3	3	Medio
Riesgo operativo	Ficheros de configuraciones	IF	Ausencia de colaborador clave	2	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Ficheros de configuraciones	IF	Debilidades de SW	3	3	Medio
Riesgo financiero	Ficheros de configuraciones	IF	Destrucción de información	2	3	Medio
Riesgo operativo	Ficheros de configuraciones	IF	Errores de operador y usuario	3	3	Medio
Riesgo tecnológico	Ficheros de configuraciones	IF	Falla técnica en SW	3	3	Medio
Riesgo financiero	Ficheros de configuraciones	IF	Filtración de información	2	3	Medio
Riesgo financiero	Ficheros de configuraciones	IF	Fraude y robo	2	3	Medio
Riesgo operativo	Ficheros de configuraciones	IF	Humedad / temperaturas elevadas	2	1	Aceptable
Riesgo financiero	Ficheros de configuraciones	IF	Incendio	1	4	Aceptable
Riesgo tecnológico	Ficheros de configuraciones	IF	Intrusión web	3	3	Medio
Riesgo financiero	Ficheros de configuraciones	IF	Inundación	1	4	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Ficheros de configuraciones	IF	Manipulación indebida de la información	3	3	Medio
Riesgo tecnológico	Ficheros de configuraciones	IF	Sniffing	3	3	Medio
Riesgo tecnológico	Ficheros de configuraciones	IF	Software malicioso	3	3	Medio
Riesgo tecnológico	Ficheros de configuraciones	IF	Uso de SW no autorizado	3	2	Medio
Riesgo financiero	Licencias servidores Linux	IF	Acceso no autorizado	1	3	Aceptable
Riesgo financiero	Licencias servidores Linux	IF	Acceso no presencial sin autorización	3	3	Medio
Riesgo operativo	Licencias servidores Linux	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Licencias servidores Linux	IF	Debilidades de SW	3	3	Medio
Riesgo financiero	Licencias servidores Linux	IF	Destrucción de información	2	2	Aceptable
Riesgo operativo	Licencias servidores Linux	IF	Errores de operador y usuario	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Licencias servidores Linux	IF	Falla técnica en SW	3	1	Aceptable
Riesgo financiero	Licencias servidores Linux	IF	Filtración de información	2	3	Medio
Riesgo financiero	Licencias servidores Linux	IF	Fraude y robo	2	3	Medio
Riesgo operativo	Licencias servidores Linux	IF	Humedad / temperaturas elevadas	2	1	Aceptable
Riesgo financiero	Licencias servidores Linux	IF	Incendio	1	2	Aceptable
Riesgo tecnológico	Licencias servidores Linux	IF	Intrusión web	3	3	Medio
Riesgo financiero	Licencias servidores Linux	IF	Inundación	1	1	Aceptable
Riesgo financiero	Licencias servidores Linux	IF	Manipulación indebida de la información	3	3	Medio
Riesgo tecnológico	Licencias servidores Linux	IF	Sniffing	3	1	Aceptable
Riesgo tecnológico	Licencias servidores Linux	IF	Software malicioso	3	3	Medio

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Licencias servidores Linux	IF	Uso de SW no autorizado	3	1	Aceptable
Riesgo financiero	Licencias Windows	IF	Acceso no autorizado	1	2	Aceptable
Riesgo financiero	Licencias Windows	IF	Acceso no presencial sin autorización	3	2	Medio
Riesgo operativo	Licencias Windows	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Licencias Windows	IF	Debilidades de SW	3	2	Medio
Riesgo financiero	Licencias Windows	IF	Destrucción de información	2	2	Aceptable
Riesgo operativo	Licencias Windows	IF	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	Licencias Windows	IF	Falla técnica en SW	3	1	Aceptable
Riesgo financiero	Licencias Windows	IF	Filtración de información	2	2	Aceptable
Riesgo financiero	Licencias Windows	IF	Fraude y robo	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Licencias Windows	IF	Humedad / temperaturas elevadas	2	1	Aceptable
Riesgo financiero	Licencias Windows	IF	Incendio	1	2	Aceptable
Riesgo tecnológico	Licencias Windows	IF	Intrusión web	3	2	Medio
Riesgo financiero	Licencias Windows	IF	Inundación	1	1	Aceptable
Riesgo financiero	Licencias Windows	IF	Manipulación indebida de la información	3	2	Medio
Riesgo tecnológico	Licencias Windows	IF	Sniffing	3	1	Aceptable
Riesgo tecnológico	Licencias Windows	IF	Software malicioso	3	2	Medio
Riesgo tecnológico	Licencias Windows	IF	Uso de SW no autorizado	3	1	Aceptable
Riesgo financiero	Manual de usuarios ERP Titanium SaaS	IF	Acceso no autorizado	1	1	Aceptable
Riesgo financiero	Manual de usuarios ERP Titanium SaaS	IF	Acceso no presencial sin autorización	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Manual de usuarios ERP Titanium SaaS	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Manual de usuarios ERP Titanium SaaS	IF	Debilidades de SW	3	1	Aceptable
Riesgo financiero	Manual de usuarios ERP Titanium SaaS	IF	Destrucción de información	2	1	Aceptable
Riesgo operativo	Manual de usuarios ERP Titanium SaaS	IF	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	Manual de usuarios ERP Titanium SaaS	IF	Falla técnica en SW	3	1	Aceptable
Riesgo financiero	Manual de usuarios ERP Titanium SaaS	IF	Filtración de información	2	1	Aceptable
Riesgo financiero	Manual de usuarios ERP Titanium SaaS	IF	Fraude y robo	2	1	Aceptable
Riesgo operativo	Manual de usuarios ERP Titanium SaaS	IF	Humedad / temperaturas elevadas	2	1	Aceptable
Riesgo financiero	Manual de usuarios ERP Titanium SaaS	IF	Incendio	1	1	Aceptable
Riesgo tecnológico	Manual de usuarios ERP Titanium SaaS	IF	Intrusión web	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Manual de usuarios ERP Titanium SaaS	IF	Inundación	1	1	Aceptable
Riesgo financiero	Manual de usuarios ERP Titanium SaaS	IF	Manipulación indebida de la información	3	1	Aceptable
Riesgo tecnológico	Manual de usuarios ERP Titanium SaaS	IF	Sniffing	3	1	Aceptable
Riesgo tecnológico	Manual de usuarios ERP Titanium SaaS	IF	Software malicioso	3	1	Aceptable
Riesgo tecnológico	Manual de usuarios ERP Titanium SaaS	IF	Uso de SW no autorizado	3	1	Aceptable
Riesgo financiero	Respaldos de base de datos	IF	Acceso no autorizado	1	2	Aceptable
Riesgo financiero	Respaldos de base de datos	IF	Acceso no presencial sin autorización	3	2	Medio
Riesgo operativo	Respaldos de base de datos	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Respaldos de base de datos	IF	Debilidades de SW	3	1	Aceptable
Riesgo financiero	Respaldos de base de datos	IF	Destrucción de información	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Respaldos de base de datos	IF	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	Respaldos de base de datos	IF	Falla técnica en SW	3	1	Aceptable
Riesgo financiero	Respaldos de base de datos	IF	Filtración de información	2	3	Medio
Riesgo financiero	Respaldos de base de datos	IF	Fraude y robo	2	2	Aceptable
Riesgo operativo	Respaldos de base de datos	IF	Humedad / temperaturas elevadas	2	2	Aceptable
Riesgo financiero	Respaldos de base de datos	IF	Incendio	1	4	Aceptable
Riesgo tecnológico	Respaldos de base de datos	IF	Intrusión web	3	3	Medio
Riesgo financiero	Respaldos de base de datos	IF	Inundación	1	4	Aceptable
Riesgo financiero	Respaldos de base de datos	IF	Manipulación indebida de la información	3	2	Medio
Riesgo tecnológico	Respaldos de base de datos	IF	Sniffing	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Respaldos de base de datos	IF	Software malicioso	3	2	Medio
Riesgo tecnológico	Respaldos de base de datos	IF	Uso de SW no autorizado	3	1	Aceptable
Riesgo financiero	Respaldos de código fuentes	IF	Acceso no autorizado	1	2	Aceptable
Riesgo financiero	Respaldos de código fuentes	IF	Acceso no presencial sin autorización	3	2	Medio
Riesgo operativo	Respaldos de código fuentes	IF	Ausencia de colaborador clave	2	1	Aceptable
Riesgo tecnológico	Respaldos de código fuentes	IF	Debilidades de SW	3	1	Aceptable
Riesgo financiero	Respaldos de código fuentes	IF	Destrucción de información	2	2	Aceptable
Riesgo operativo	Respaldos de código fuentes	IF	Errores de operador y usuario	3	1	Aceptable
Riesgo tecnológico	Respaldos de código fuentes	IF	Falla técnica en SW	3	1	Aceptable
Riesgo financiero	Respaldos de código fuentes	IF	Filtración de información	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Respaldos de código fuentes	IF	Fraude y robo	2	2	Aceptable
Riesgo operativo	Respaldos de código fuentes	IF	Humedad / temperaturas elevadas	2	2	Aceptable
Riesgo financiero	Respaldos de código fuentes	IF	Incendio	1	4	Aceptable
Riesgo tecnológico	Respaldos de código fuentes	IF	Intrusión web	3	3	Medio
Riesgo financiero	Respaldos de código fuentes	IF	Inundación	1	4	Aceptable
Riesgo financiero	Respaldos de código fuentes	IF	Manipulación indebida de la información	3	2	Medio
Riesgo tecnológico	Respaldos de código fuentes	IF	Sniffing	3	1	Aceptable
Riesgo tecnológico	Respaldos de código fuentes	IF	Software malicioso	3	2	Medio
Riesgo tecnológico	Respaldos de código fuentes	IF	Uso de SW no autorizado	3	1	Aceptable
Riesgo financiero	Oficinas Negysert	IN	Sabotaje	1	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Oficinas Negysert	IN	Inundación	1	4	Aceptable
Riesgo financiero	Oficinas Negysert	IN	Incendio	1	4	Aceptable
Riesgo operativo	Usuarios externos	PE	Ausencia de colaborador clave	2	1	Aceptable
Riesgo financiero	Usuarios externos	PE	Corrupción	2	2	Aceptable
Riesgo financiero	Usuarios externos	PE	Filtración de información	2	2	Aceptable
Riesgo financiero	Usuarios externos	PE	Fraude y robo	2	2	Aceptable
Riesgo financiero	Usuarios externos	PE	Incendio	1	4	Aceptable
Riesgo financiero	Usuarios externos	PE	Ingeniería social	3	2	Medio
Riesgo financiero	Usuarios externos	PE	Manipulación indebida de la información	3	2	Medio
Riesgo financiero	Usuarios externos	PE	Personal no idóneo	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Usuarios internos	PE	Ausencia de colaborador clave	2	2	Aceptable
Riesgo financiero	Usuarios internos	PE	Corrupción	2	3	Medio
Riesgo financiero	Usuarios internos	PE	Filtración de información	2	3	Medio
Riesgo financiero	Usuarios internos	PE	Fraude y robo	2	3	Medio
Riesgo financiero	Usuarios internos	PE	Incendio	1	4	Aceptable
Riesgo financiero	Usuarios internos	PE	Ingeniería social	3	3	Medio
Riesgo financiero	Usuarios internos	PE	Manipulación indebida de la información	2	3	Medio
Riesgo financiero	Usuarios internos	PE	Personal no idóneo	2	2	Aceptable
Riesgo operativo	Personal de operaciones SaaS	PE	Ausencia de colaborador clave	2	2	Aceptable
Riesgo financiero	Personal de operaciones SaaS	PE	Corrupción	2	3	Medio

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Personal de operaciones SaaS	PE	Filtración de información	2	3	Medio
Riesgo financiero	Personal de operaciones SaaS	PE	Fraude y robo	2	3	Medio
Riesgo financiero	Personal de operaciones SaaS	PE	Incendio	1	4	Aceptable
Riesgo financiero	Personal de operaciones SaaS	PE	Ingeniería social	3	3	Medio
Riesgo financiero	Personal de operaciones SaaS	PE	Manipulación indebida de la información	3	3	Medio
Riesgo financiero	Personal de operaciones SaaS	PE	Personal no idóneo	2	2	Aceptable
Riesgo tecnológico	Internet corporativo	SE	Denegación de servicios	2	3	Medio
Riesgo tecnológico	Internet corporativo	SE	Deterioro de servicios provistos por terceros	2	3	Medio
Riesgo financiero	Internet corporativo	SE	Ingeniería social	1	1	Aceptable
Riesgo financiero	Internet corporativo	SE	Manipulación indebida de la información	1	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Internet corporativo	SE	Recuperación extemporánea de servicios	2	3	Medio
Riesgo financiero	Internet corporativo	SE	Sabotaje	2	2	Aceptable
Riesgo tecnológico	Servicio de correo electrónico	SE	Denegación de servicios	2	2	Aceptable
Riesgo tecnológico	Servicio de correo electrónico	SE	Deterioro de servicios provistos por terceros	2	2	Aceptable
Riesgo financiero	Servicio de correo electrónico	SE	Ingeniería social	1	1	Aceptable
Riesgo financiero	Servicio de correo electrónico	SE	Manipulación indebida de la información	1	1	Aceptable
Riesgo tecnológico	Servicio de correo electrónico	SE	Recuperación extemporánea de servicios	2	2	Aceptable
Riesgo financiero	Servicio de correo electrónico	SE	Sabotaje	2	2	Aceptable
Riesgo financiero	Sistema Antivirus	SW	Acceso no presencial sin autorización	2	2	Aceptable
Riesgo tecnológico	Sistema Antivirus	SW	Problemas con los servicios de comunicación	2	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Sistema Antivirus	SW	Falla técnica en SW	2	2	Aceptable
Riesgo financiero	Sistema Antivirus	SW	Acceso no autorizado	1	2	Aceptable
Riesgo financiero	Sistema Antivirus	SW	Manipulación indebida de la información	2	2	Aceptable
Riesgo tecnológico	Sistema Antivirus	SW	Debilidades de SW	2	2	Aceptable
Riesgo tecnológico	Sistema Antivirus	SW	Uso de SW no autorizado	2	2	Aceptable
Riesgo operativo	Sistema Antivirus	SW	Errores de operador y usuario	2	1	Aceptable
Riesgo financiero	Sistema Antivirus	SW	Fraude y robo	2	1	Aceptable
Riesgo tecnológico	Sistema Antivirus	SW	Intrusión web	3	2	Medio
Riesgo operativo	Sistema Antivirus	SW	Ausencia de colaborador clave	2	1	Aceptable
Riesgo financiero	Sistema Antivirus	SW	Incendio	1	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Integración sistema facturador combustibles	SW	Acceso no presencial sin autorización	2	2	Aceptable
Riesgo tecnológico	Integración sistema facturador combustibles	SW	Problemas con los servicios de comunicación	2	2	Aceptable
Riesgo tecnológico	Integración sistema facturador combustibles	SW	Falla técnica en SW	2	2	Aceptable
Riesgo financiero	Integración sistema facturador combustibles	SW	Acceso no autorizado	2	1	Aceptable
Riesgo financiero	Integración sistema facturador combustibles	SW	Manipulación indebida de la información	2	2	Aceptable
Riesgo tecnológico	Integración sistema facturador combustibles	SW	Debilidades de SW	2	2	Aceptable
Riesgo tecnológico	Integración sistema facturador combustibles	SW	Uso de SW no autorizado	2	2	Aceptable
Riesgo operativo	Integración sistema facturador combustibles	SW	Errores de operador y usuario	2	1	Aceptable
Riesgo financiero	Integración sistema facturador combustibles	SW	Fraude y robo	2	1	Aceptable
Riesgo tecnológico	Integración sistema facturador combustibles	SW	Intrusión web	3	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Integración sistema facturador combustibles	SW	Ausencia de colaborador clave	2	1	Aceptable
Riesgo financiero	Integración sistema facturador combustibles	SW	Incendio	1	2	Aceptable
Riesgo financiero	Hipervisor de máquinas virtuales	SW	Acceso no presencial sin autorización	2	3	Medio
Riesgo tecnológico	Hipervisor de máquinas virtuales	SW	Problemas con los servicios de comunicación	2	3	Medio
Riesgo tecnológico	Hipervisor de máquinas virtuales	SW	Falla técnica en SW	2	3	Medio
Riesgo financiero	Hipervisor de máquinas virtuales	SW	Acceso no autorizado	1	3	Aceptable
Riesgo financiero	Hipervisor de máquinas virtuales	SW	Manipulación indebida de la información	2	3	Medio
Riesgo tecnológico	Hipervisor de máquinas virtuales	SW	Debilidades de SW	2	3	Medio
Riesgo tecnológico	Hipervisor de máquinas virtuales	SW	Uso de SW no autorizado	2	3	Medio
Riesgo operativo	Hipervisor de máquinas virtuales	SW	Errores de operador y usuario	2	1	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Hipervisor de máquinas virtuales	SW	Fraude y robo	2	2	Aceptable
Riesgo tecnológico	Hipervisor de máquinas virtuales	SW	Intrusión web	3	3	Medio
Riesgo operativo	Hipervisor de máquinas virtuales	SW	Ausencia de colaborador clave	2	2	Aceptable
Riesgo financiero	Hipervisor de máquinas virtuales	SW	Incendio	1	3	Aceptable
Riesgo financiero	Ofimática	SW	Acceso no presencial sin autorización	2	2	Aceptable
Riesgo tecnológico	Ofimática	SW	Problemas con los servicios de comunicación	2	1	Aceptable
Riesgo tecnológico	Ofimática	SW	Falla técnica en SW	1	2	Aceptable
Riesgo financiero	Ofimática	SW	Acceso no autorizado	1	2	Aceptable
Riesgo financiero	Ofimática	SW	Manipulación indebida de la información	2	2	Aceptable
Riesgo tecnológico	Ofimática	SW	Debilidades de SW	1	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Ofimática	SW	Uso de SW no autorizado	2	1	Aceptable
Riesgo operativo	Ofimática	SW	Errores de operador y usuario	2	2	Aceptable
Riesgo financiero	Ofimática	SW	Fraude y robo	2	2	Aceptable
Riesgo tecnológico	Ofimática	SW	Intrusión web	2	2	Aceptable
Riesgo operativo	Ofimática	SW	Ausencia de colaborador clave	2	1	Aceptable
Riesgo financiero	Ofimática	SW	Incendio	1	3	Aceptable
Riesgo financiero	Servidor virtual de Aplication Server	SW	Acceso no presencial sin autorización	2	4	Medio
Riesgo tecnológico	Servidor virtual de Aplication Server	SW	Problemas con los servicios de comunicación	2	3	Medio
Riesgo tecnológico	Servidor virtual de Aplication Server	SW	Falla técnica en SW	2	3	Medio
Riesgo financiero	Servidor virtual de Aplication Server	SW	Acceso no autorizado	2	4	Medio

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Servidor virtual de Aplication Server	SW	Manipulación indebida de la información	2	4	Medio
Riesgo tecnológico	Servidor virtual de Aplication Server	SW	Debilidades de SW	2	3	Medio
Riesgo tecnológico	Servidor virtual de Aplication Server	SW	Uso de SW no autorizado	1	4	Aceptable
Riesgo operativo	Servidor virtual de Aplication Server	SW	Errores de operador y usuario	2	2	Aceptable
Riesgo financiero	Servidor virtual de Aplication Server	SW	Fraude y robo	2	2	Aceptable
Riesgo tecnológico	Servidor virtual de Aplication Server	SW	Intrusión web	3	3	Medio
Riesgo operativo	Servidor virtual de Aplication Server	SW	Ausencia de colaborador clave	2	2	Aceptable
Riesgo financiero	Servidor virtual de Aplication Server	SW	Incendio	1	3	Aceptable
Riesgo financiero	Servidor virtual de base de datos	SW	Acceso no presencial sin autorización	2	4	Medio
Riesgo tecnológico	Servidor virtual de base de datos	SW	Problemas con los servicios de comunicación	2	3	Medio

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo tecnológico	Servidor virtual de base de datos	SW	Falla técnica en SW	2	3	Medio
Riesgo financiero	Servidor virtual de base de datos	SW	Acceso no autorizado	2	4	Medio
Riesgo financiero	Servidor virtual de base de datos	SW	Manipulación indebida de la información	2	4	Medio
Riesgo tecnológico	Servidor virtual de base de datos	SW	Debilidades de SW	2	3	Medio
Riesgo tecnológico	Servidor virtual de base de datos	SW	Uso de SW no autorizado	1	4	Aceptable
Riesgo operativo	Servidor virtual de base de datos	SW	Errores de operador y usuario	2	2	Aceptable
Riesgo financiero	Servidor virtual de base de datos	SW	Fraude y robo	2	2	Aceptable
Riesgo tecnológico	Servidor virtual de base de datos	SW	Intrusión web	3	3	Medio
Riesgo operativo	Servidor virtual de base de datos	SW	Ausencia de colaborador clave	2	2	Aceptable
Riesgo financiero	Servidor virtual de base de datos	SW	Incendio	1	3	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo financiero	Integración SRI	SW	Acceso no presencial sin autorización	2	2	Aceptable
Riesgo tecnológico	Integración SRI	SW	Problemas con los servicios de comunicación	2	2	Aceptable
Riesgo tecnológico	Integración SRI	SW	Falla técnica en SW	2	2	Aceptable
Riesgo financiero	Integración SRI	SW	Acceso no autorizado	2	2	Aceptable
Riesgo financiero	Integración SRI	SW	Manipulación indebida de la información	2	2	Aceptable
Riesgo tecnológico	Integración SRI	SW	Debilidades de SW	2	2	Aceptable
Riesgo tecnológico	Integración SRI	SW	Uso de SW no autorizado	1	2	Aceptable
Riesgo operativo	Integración SRI	SW	Errores de operador y usuario	2	2	Aceptable
Riesgo financiero	Integración SRI	SW	Fraude y robo	1	2	Aceptable
Riesgo tecnológico	Integración SRI	SW	Intrusión web	2	2	Aceptable

ANEXO E - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS						
Tipo de riesgo	**Activo**	**Tipo Activo**	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Riesgo operativo	Integración SRI	SW	Ausencia de colaborador clave	2	2	Aceptable
Riesgo financiero	Integración SRI	SW	Incendio	1	2	Aceptable

ANEXO F - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS – POST IMPLEMENTACIÓN DE CONTROLES									
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**	**Tratamiento**	**Control**	**Probabilidad**	**Impacto**	**Riesgo**
Credenciales de administración	Acceso no presencial sin autorización	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 9.2.4 Gestión de la información de autenticación secreta de los usuarios 9.3.1 Uso de la información de autenticación secreta 10.1.2 Gestión de claves 12.1.1 Documentación de procedimientos de operación	2	2	Aceptable
Esquemas de base de datos por cliente	Acceso no presencial sin autorización	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 9.2.4 Gestión de la información de autenticación secreta de los usuarios 9.3.1 Uso de la información de autenticación secreta 12.1.1 Documentación de procedimientos de operación	2	2	Aceptable
Servidor de aplicaciones	Datos accedidos sin autorización	4	3	Alto	Mitigar	9.1.1 Política de control de acceso 9.2.4 Gestión de la información de autenticación secreta de los usuarios 9.3.1 Uso de la información de autenticación secreta 12.1.1 Documentación de procedimientos de operación	3	3	Medio

ANEXO F - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS – POST IMPLEMENTACIÓN DE CONTROLES									
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**	**Tratamiento**	**Control**	**Probabilidad**	**Impacto**	**Riesgo**
Servidor de base de datos	Datos accedidos sin autorización	4	3	Alto	Mitigar	9.1.1 Política de control de acceso 9.2.4 Gestión de la información de autenticación secreta de los usuarios 9.3.1 Uso de la información de autenticación secreta 12.1.1 Documentación de procedimientos de operación	3	2	Medio
Servidor web	Datos accedidos sin autorización	4	3	Alto	Mitigar	9.1.1 Política de control de acceso 9.2.4 Gestión de la información de autenticación secreta de los usuarios 9.3.1 Uso de la información de autenticación secreta 12.1.1 Documentación de procedimientos de operación	3	2	Medio
Credenciales de administración	Debilidades de SW	3	3	Medio	Mitigar	10.1.2 Gestión de claves 14.1.1 Análisis y especificación de los requisitos de seguridad 14.2.1 Política de desarrollo seguro 14.2.2 Procedimiento de control de cambio del sistema	2	2	Aceptable

ANEXO F - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS – POST IMPLEMENTACIÓN DE CONTROLES									
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**	**Tratamiento**	**Control**	**Probabilidad**	**Impacto**	**Riesgo**
Servidor web	Destrucción de información	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información 13.2.1 Políticas y procedimientos de intercambio de información 18.1.3 Protección de los registros de la organización	2	2	Aceptable
Esquemas de base de datos por cliente	Errores de operador y usuario	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 12.1.1 Documentación de procedimientos de operación 12.3.1 Respaldo de la información	2	2	Aceptable
Esquemas de base de datos por cliente	Falla técnica en SW	3	3	Medio	Mitigar	12.3.1 Respaldo de la información 14.1.1 Análisis y especificación de los requisitos de seguridad 14.2.1 Política de desarrollo seguro 14.2.2 Procedimiento de control de cambio del sistema	2	2	Aceptable

ANEXO F - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS – POST IMPLEMENTACIÓN DE CONTROLES									
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**	**Tratamiento**	**Control**	**Probabilidad**	**Impacto**	**Riesgo**
Esquemas de base de datos por cliente	Intrusión web	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información 14.1.1 Análisis y especificación de los requisitos de seguridad 14.2.1 Política de desarrollo seguro 14.2.2 Procedimiento de control de cambio del sistema	2	2	Aceptable
Hipervisor de máquinas virtuales	Intrusión web	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información	2	2	Aceptab
Servidor virtual de Aplication Server	Intrusión web	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información	2	2	Aceptable
Servidor virtual de base de datos	Intrusión web	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información	2	2	Aceptab

ANEXO F - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS – POST IMPLEMENTACIÓN DE CONTROLES									
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**	**Tratamiento**	**Control**	**Probabilidad**	**Impacto**	**Riesgo**
Esquemas de base de datos por cliente	Manipulación indebida de la información	3	3	Medio	Mitigar	9.1.1 Política de control de acceso 12.3.1 Respaldo de la información 13.2.1 Políticas y procedimientos de intercambio de información 18.1.3 Protección de los registros de la organización	2	2	Aceptable
Credenciales de administración	Sniffing	3	3	Medio	Mitigar	10.1.1 Política sobre el empleo de controles criptográficos 10.1.2 Gestión de claves 13.2.1 Políticas y procedimientos de intercambio de información	2	2	Aceptable
Esquemas de base de datos por cliente	Sniffing	3	3	Medio	Mitigar	10.1.1 Política sobre el empleo de controles criptográficos 10.1.2 Gestión de claves 13.2.1 Políticas y procedimientos de intercambio de información	2	2	Aceptable
Equipo firewall	Software malicioso	3	3	Medio	Mitigar	7.2.2 Concientización, educación y formación en seguridad de la información 8.1.3 Uso aceptable de los activos 12.2.1 Controles ante software malicioso 12.6.2 Restricciones en la instalación de software	2	2	Aceptable

ANEXO F - ANÁLISIS Y VALORACIÓN DE LOS RIESGOS – POST IMPLEMENTACIÓN DE CONTROLES									
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**	**Tratamiento**	**Control**	**Probabilidad**	**Impacto**	**Riesgo**
Servidor de aplicaciones	Software malicioso	4	3	Alto	Mitigar	7.2.2 Concientización, educación y formación en seguridad de la información 8.1.3 Uso aceptable de los activos 12.2.1 Controles ante software malicioso 12.6.2 Restricciones en la instalación de software	3	2	Medio
Servidor de base de datos	Software malicioso	4	3	Alto	Mitigar	7.2.2 Concientización, educación y formación en seguridad de la información 8.1.3 Uso aceptable de los activos 12.2.1 Controles ante software malicioso 12.6.2 Restricciones en la instalación de software	3	2	Medio
Servidor web	Software malicioso	4	3	Alto	Mitigar	7.2.2 Concientización, educación y formación en seguridad de la información 8.1.3 Uso aceptable de los activos 12.2.1 Controles ante software malicioso 12.6.2 Restricciones en la instalación de software	3	2	Medio
Esquemas de base de datos por cliente	Software malicioso	4	3	Alto	Mitigar	7.2.2 Concientización, educación y formación en seguridad de la información 8.1.3 Uso aceptable de los activos 12.2.1 Controles ante software malicioso 12.6.2 Restricciones en la instalación de software	3	2	Medio

ANEXO G: Detalles del Cronograma

Nombre de tarea	Duración	Comienzo	Fin	Costo
Esquema de seguridad ISO 27001	**290 días**	**lun 26/7/21**	**vie 2/9/22**	**$6.449,00**
Análisis de brechas GAP	12 días	lun 26/7/21	mar 10/8/21	$148,80
Análisis del contexto de la organización	10 días	mié 11/8/21	mar 24/8/21	$124,00
Planificación del Esquema	**68 días**	**mié 25/8/21**	**vie 26/11/21**	**$843,20**
Inventario de activos	8 días	mié 25/8/21	vie 3/9/21	$99,20
Catálogo de Amenazas	20 días	lun 6/9/21	vie 1/10/21	$248,00
Valoración de las amenazas	10 días	lun 4/10/21	vie 15/10/21	$124,00
Determinación de objetivos del SGSI	2 días	lun 18/10/21	mar 19/10/21	$24,80
Análisis de riesgos	12 días	mié 20/10/21	jue 4/11/21	$148,80
Evaluación de riesgos	8 días	vie 5/11/21	mar 16/11/21	$99,20
Plan de tratamiento de riesgos	2 días	mié 17/11/21	jue 18/11/21	$24,80
Selección de controles	6 días	vie 19/11/21	vie 26/11/21	$74,40
Elaboración de las políticas	40 días	lun 29/11/21	vie 21/1/22	$496,00
Documentación del esquema	**85 días**	**lun 24/1/22**	**vie 20/5/22**	**$1.440,00**
Políticas de seguridad	30 días	lun 24/1/22	vie 4/3/22	$372,00
Procesos de seguridad	20 días	lun 7/3/22	vie 1/4/22	$248,00
Instrucciones técnicas de seguridad	15 días	lun 4/4/22	vie 22/4/22	$186,00
Registros y evidencias	10 días	lun 25/4/22	vie 6/5/22	$124,00
Definición de funciones y responsabilidades de seguridad	10 días	lun 9/5/22	vie 20/5/22	$510,00
Implementación del esquema	**33 días**	**lun 23/5/22**	**mié 6/7/22**	**$409,20**
Establecimiento de criterios de medición para los controles	10 días	lun 23/5/22	vie 3/6/22	$124,00
Establecimiento de valores meta	5 días	lun 6/6/22	vie 10/6/22	$62,00
Establecimiento de formas de cálculo	3 días	lun 13/6/22	mié 15/6/22	$37,20
Establecimiento de proceso de mejora continua	15 días	jue 16/6/22	mié 6/7/22	$186,00
Comunicación y sensibilización	10 días	jue 7/7/22	mié 20/7/22	$634,00
Auditoría interna según ISO 27001	12 días	jue 21/7/22	vie 5/8/22	$148,80
Revisión por la dirección según ISO 27001	5 días	lun 8/8/22	vie 12/8/22	$405,00
Proceso de certificación ISO 27001	15 días	lun 15/8/22	vie 2/9/22	$1.800,00

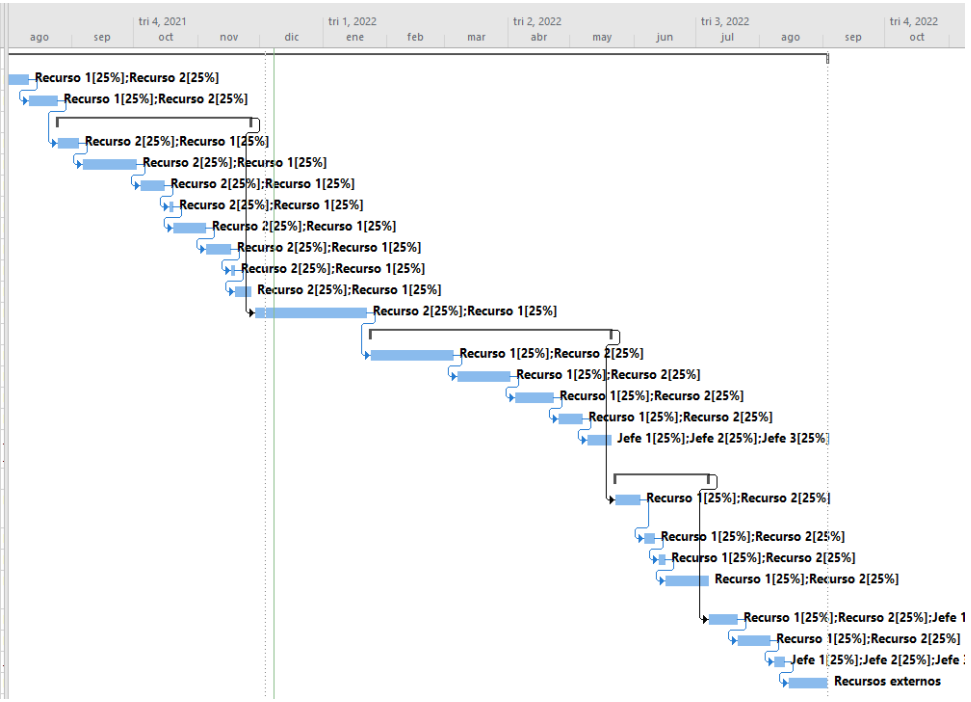


Imagen 1 Diagrama Gantt
Fuente: Autor

Nombre de tarea	Trabajo	Duración	Comienzo	Fin	Detalles	tri 3, 2021 jul	ago	sep	tri 4, 2021 oct	nov	dic	tri 1, 2022 ene
Esquema de seguridad ISO 27001	**1.320 horas**	**290 días**	**lun 26/7/21**	**vie 2/**	Trab.	20h	88h	88h	84h	88h	92h	84h
Análisis de brechas GAP	48 horas	12 días	lun 26/7/21	mar 10/	Trab.	20h	28h					
Recurso 1	*24 horas*		*lun 26/7/21*	*mar 10/*	Trab.	10h	14h					
Recurso 2	*24 horas*		*lun 26/7/21*	*mar 10/*	Trab.	10h	14h					
Análisis del contexto de la organización	40 horas	10 días	mié 11/8/21	mar 24/	Trab.		40h					
Recurso 1	*20 horas*		*mié 11/8/21*	*mar 24/*	Trab.		20h					
Recurso 2	*20 horas*		*mié 11/8/21*	*mar 24/*	Trab.		20h					
Planificación del Esquema	**272 horas**	**68 días**	**mié 25/8/21**	**vie 26/1**	Trab.		20h	88h	84h	80h		
Inventario de activos	32 horas	8 días	mié 25/8/21	vie 3/	Trab.		20h	12h				
Recurso 1	*16 horas*		*mié 25/8/21*	*vie 3/*	Trab.		10h	6h				
Recurso 2	*16 horas*		*mié 25/8/21*	*vie 3/*	Trab.		10h	6h				
Catálogo de Amenazas	80 horas	20 días	lun 6/9/21	vie 1/1	Trab.			76h	4h			
Recurso 1	*40 horas*		*lun 6/9/21*	*vie 1/1*	Trab.			38h	2h			
Recurso 2	*40 horas*		*lun 6/9/21*	*vie 1/1*	Trab.			38h	2h			
Valoración de las amenazas	40 horas	10 días	lun 4/10/21	vie 15/1	Trab.				40h			
Recurso 1	*20 horas*		*lun 4/10/21*	*vie 15/1*	Trab.				20h			
Recurso 2	*20 horas*		*lun 4/10/21*	*vie 15/1*	Trab.				20h			
Determinación de objetivos del SGSI	8 horas	2 días	lun 18/10/21	mar 19/1	Trab.				8h			
Recurso 1	*4 horas*		*lun 18/10/21*	*mar 19/1*	Trab.				4h			
Recurso 2	*4 horas*		*lun 18/10/21*	*mar 19/1*	Trab.				4h			
Análisis de riesgos	48 horas	12 días	mié 20/10/21	jue 4/1	Trab.				32h	16h		
Recurso 1	*24 horas*		*mié 20/10/21*	*jue 4/1*	Trab.				16h	8h		
Recurso 2	*24 horas*		*mié 20/10/21*	*jue 4/1*	Trab.				16h	8h		
Evaluación de riesgos	32 horas	8 días	vie 5/11/21	mar 16/1	Trab.					32h		
Recurso 1	*16 horas*		*vie 5/11/21*	*mar 16/1*	Trab.					16h		
Recurso 2	*16 horas*		*vie 5/11/21*	*mar 16/1*	Trab.					16h		
Plan de tratamiento de riesgos	8 horas	2 días	mié 17/11/21	jue 18/1	Trab.					8h		
Recurso 1	*4 horas*		*mié 17/11/21*	*jue 18/1*	Trab.					4h		
Recurso 2	*4 horas*		*mié 17/11/21*	*jue 18/1*	Trab.					4h		
Selección de controles	24 horas	6 días	vie 19/11/21	vie 26/1	Trab.					24h		
Recurso 1	*12 horas*		*vie 19/11/21*	*vie 26/1*	Trab.					12h		
Recurso 2	*12 horas*		*vie 19/11/21*	*vie 26/1*	Trab.					12h		
Elaboración de las políticas	160 horas	40 días	lun 29/11/21	vie 21/	Trab.					8h	92h	60h
Recurso 1	*80 horas*		*lun 29/11/21*	*vie 21/*	Trab.					4h	46h	30h
Recurso 2	*80 horas*		*lun 29/11/21*	*vie 21/*	Trab.					4h	46h	30h

Imagen 2 Uso de tareas
Fuente: Autor

Nombre de tarea	Trabajo	Duración	Comienzo	Fin	Detalles	tri 1, 2022 ene	feb	mar	tri 2, 2022 abr	may	jun
Documentación del esquema	**360 horas**	**85 días**	**lun 24/1/22**	**vie 20/**	Trab.	24h	80h	92h	84h	80h	
Políticas de seguridad	120 horas	30 días	lun 24/1/22	vie 4/	Trab.	24h	80h	16h			
Recurso 1	*60 horas*		*lun 24/1/22*	*vie 4/*	Trab.	12h	40h	8h			
Recurso 2	*60 horas*		*lun 24/1/22*	*vie 4/*	Trab.	12h	40h	8h			
Procesos de seguridad	80 horas	20 días	lun 7/3/22	vie 1/	Trab.			76h	4h		
Recurso 1	*40 horas*		*lun 7/3/22*	*vie 1/*	Trab.			38h	2h		
Recurso 2	*40 horas*		*lun 7/3/22*	*vie 1/*	Trab.			38h	2h		
Instrucciones técnicas de seguridad	60 horas	15 días	lun 4/4/22	vie 22/	Trab.				60h		
Recurso 1	*30 horas*		*lun 4/4/22*	*vie 22/*	Trab.				30h		
Recurso 2	*30 horas*		*lun 4/4/22*	*vie 22/*	Trab.				30h		
Registros y evidencias	40 horas	10 días	lun 25/4/22	vie 6/	Trab.				20h	20h	
Recurso 1	*20 horas*		*lun 25/4/22*	*vie 6/*	Trab.				10h	10h	
Recurso 2	*20 horas*		*lun 25/4/22*	*vie 6/*	Trab.				10h	10h	
Definición de funciones y responsabilidades de seguridad	60 horas	10 días	lun 9/5/22	vie 20/	Trab.					60h	
Jefe 1	*20 horas*		*lun 9/5/22*	*vie 20/*	Trab.					20h	
Jefe 2	*20 horas*		*lun 9/5/22*	*vie 20/*	Trab.					20h	
Jefe 3	*20 horas*		*lun 9/5/22*	*vie 20/*	Trab.					20h	

Imagen 3 Uso de tareas
Fuente: Autor

Nombre de tarea	Trabajo	Duración	Comienzo	Fin	Detalles	22 may	jun	tri 3, 2022 jul	ago	sep
Implementación del esquema	**132 horas**	**33 días**	**lun 23/5/22**	**mié 6/**	Trab.	28h	88h	16h		
Establecimiento de criterios de medición para los controles	40 horas	10 días	lun 23/5/22	vie 3/	Trab.	28h	12h			
Recurso 1	*20 horas*		*lun 23/5/22*	*vie 3/*	Trab.	14h	6h			
Recurso 2	*20 horas*		*lun 23/5/22*	*vie 3/*	Trab.	14h	6h			
Establecimiento de valores meta	20 horas	5 días	lun 6/6/22	vie 10/	Trab.		20h			
Recurso 1	*10 horas*		*lun 6/6/22*	*vie 10/*	Trab.		10h			
Recurso 2	*10 horas*		*lun 6/6/22*	*vie 10/*	Trab.		10h			
Establecimiento de formas de cálculo	12 horas	3 días	lun 13/6/22	mié 15/	Trab.		12h			
Recurso 1	*6 horas*		*lun 13/6/22*	*mié 15/*	Trab.		6h			
Recurso 2	*6 horas*		*lun 13/6/22*	*mié 15/*	Trab.		6h			
Establecimiento de proceso de mejora continua	60 horas	15 días	jue 16/6/22	mié 6/	Trab.		44h	16h		
Recurso 1	*30 horas*		*jue 16/6/22*	*mié 6/*	Trab.		22h	8h		
Recurso 2	*30 horas*		*jue 16/6/22*	*mié 6/*	Trab.		22h	8h		
Comunicación y sensibilización	100 horas	10 días	jue 7/7/22	mié 20/	Trab.			100h		
Recurso 1	*20 horas*		*jue 7/7/22*	*mié 20/*	Trab.			20h		
Recurso 2	*20 horas*		*jue 7/7/22*	*mié 20/*	Trab.			20h		
Jefe 1	*20 horas*		*jue 7/7/22*	*mié 20/*	Trab.			20h		
Jefe 2	*20 horas*		*jue 7/7/22*	*mié 20/*	Trab.			20h		
Jefe 3	*20 horas*		*jue 7/7/22*	*mié 20/*	Trab.			20h		
Auditoría interna según ISO 27001	48 horas	12 días	jue 21/7/22	vie 5/	Trab.			28h	20h	
Recurso 1	*24 horas*		*jue 21/7/22*	*vie 5/*	Trab.			14h	10h	
Recurso 2	*24 horas*		*jue 21/7/22*	*vie 5/*	Trab.			14h	10h	
Revisión por la dirección según ISO 27001	40 horas	5 días	lun 8/8/22	vie 12/	Trab.				40h	
Jefe 1	*10 horas*		*lun 8/8/22*	*vie 12/*	Trab.				10h	
Jefe 2	*10 horas*		*lun 8/8/22*	*vie 12/*	Trab.				10h	
Jefe 3	*10 horas*		*lun 8/8/22*	*vie 12/*	Trab.				10h	
Presidente	*10 horas*		*lun 8/8/22*	*vie 12/*	Trab.				10h	
Proceso de certificación ISO 27001	120 horas	15 días	lun 15/8/22	vie 2/	Trab.				104h	16h
Recursos externos	*120 horas*		*lun 15/8/22*	*vie 2/*	Trab.				104h	16h

Imagen 4 Uso de tareas
Fuente: Autor